NetOp® Netfilter

get the full picture

Version 5.0

Benutzerhandbuch



Bitte richten Sie Ihre Anmerkungen an:
Danware Data A/S
Bregnerodvej 127
DK-3460 Birkerod
Dänemark
Fax: +45 45 90 25 26
E-Mail: info@netop.com
Internet: www.netop.com

Inhalt

1 Einführung

NetOp Netfilter Admin ist ein Tool für die Verwaltung und Wartung von NetOp Netfilter-Servern. Bei dem von Danware A/S entwickelten NetOp Netfilter handelt es sich um einen leistungsfähigen Internet-Filter.

Sollten bei der Nutzung dieses Produkts Probleme auftreten, schlagen Sie zunächst im vorliegenden Benutzerhandbuch nach. Weitere Anleitungen zur Fehlerbehebung finden Sie unter help.netop.com in Form einer "KnowledgeBase", die detaillierte technische Daten enthält.

Über Ihren NetOp-Händler vor Ort erhalten Sie weitere Informationen darüber, wie Sie Ihr NetOp-Produkt optimal nutzen können.

Konnten Sie mit den vorherigen Schritten keine Abhilfe schaffen, senden Sie eine Support-Anfrage direkt an den NetOp-Support. Verwenden Sie dazu das Formular "Technischen Support kontaktieren", das Sie unter www.netop.com im Bereich "Support" finden. Wir sind bemüht, Ihnen schnellstmöglich eine Lösung des Problems zu liefern.

Eine Anleitung zur Verwendung der Hilfeseiten von Netfilter Admin finden Sie unter Übersicht.

Support- und Kontaktinformationen finden Sie auf der Seite Kontaktinformationen.

NetOp Support-Team

1.1 Funktionen

Pornografie und Glücksspiel zählen zu den am schnellsten wachsenden und profitabelsten Bereichen im Internet.

Für Unternehmen kann der einfache Zugriff auf Pornografie, Glücksspiel und andere unangemessene Inhalte von den internen Computern aus zu geringerer Produktivität, höherer Belastung des Unternehmensnetzwerks, Risiken hinsichtlich sexueller Belästigung sowie zur Beschädigung des guten Rufs des Unternehmens führen.

Schulen und Bibliotheken, die Schülern und anderen Benutzern Zugang zum Internet ermöglichen, haben die moralische Verpflichtung, Minderjährige vor unangemessenen Inhalten zu schützen. Gleichzeitig sind diese Anbieter verpflichtet sicherzustellen, dass der Internet-Zugang nicht verwendet wird, um beispielsweise das Urheberrecht an Musik, Filmen oder Software zu verletzen. Durch Filterung des Internet-Zugriffs mit Hilfe von NetOp Netfilter kann die unzweckmäßige und illegale Internet-Nutzung deutlich reduziert werden.

NetOp Netfilter kann unangemessene Internet-Inhalte aus folgenden Kategorien sperren:

- Pornografie
- Glücksspiel
- Dating
- Hass, Rassismus und Diskriminierung
- Gewalt und vulgärer Humor
- Illegale oder gefährliche Aktivitäten
- Urheberrechtsverletzungen (Piraterie)

NetOp Netfilter basiert auf einem innovativen Filteralgorithmus, mit dem Bilder und Text der besuchten Seiten analysiert werden. Wird eine Webseite als unangemessen eingestuft, erscheint anstelle dieser Seite eine Warnmeldung, dass es sich möglicherweise um unerwünschte Inhalte handelt. Der Administrator kann angeben, ob die Benutzer nach einer Warnung die betreffende Seite anzeigen oder lediglich zur vorherigen Seite zurückkehren können. Entscheidet sich ein Benutzer, eine Seite trotz vorheriger Warnung anzuzeigen, wird diese in einer Protokolldatei registriert.

NetOp Netfilter kann außerdem Chats, Peer-to-Peer-Programme und Streaming-Medien (Audio und Video) sperren und das Herunterladen von MP3-Dateien oder großen Dateien wie Filmen oder Software protokollieren. Zusätzlich kann das Herunterladen von Dateien mit bestimmten Namen/Erweiterungen gesperrt werden.

NetOp Netfilter agiert als Proxy-Server für den HTTP-Datenverkehr. Auf diese Weise ist die Kompatibilität mit nahezu allen Web-Browsern und Betriebssystemen gewährleistet.

NetOp Netfilter kann eigenständig verwendet werden (siehe Abbildung 1) und lässt sich auch gemeinsam mit einem externen Proxy-Server einsetzen (siehe Abbildung 2). Durch die Möglichkeit, NetOp Netfilter mit dem Proxy-Server eines anderen Anbieters zu kombinieren, wird sichergestellt, dass sich NetOp Netfilter problemlos in ein vorhandenes Netzwerk integrieren lässt.

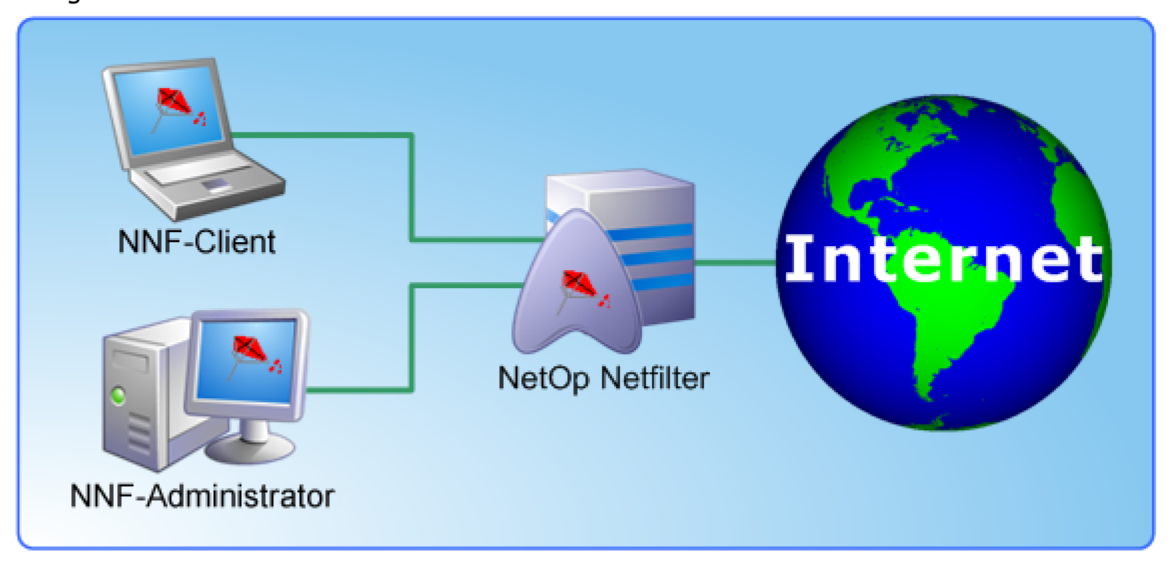


Abbildung 1: Nutzung von NetOp Netfilter ohne Proxy-Server eines anderen Anbieters.

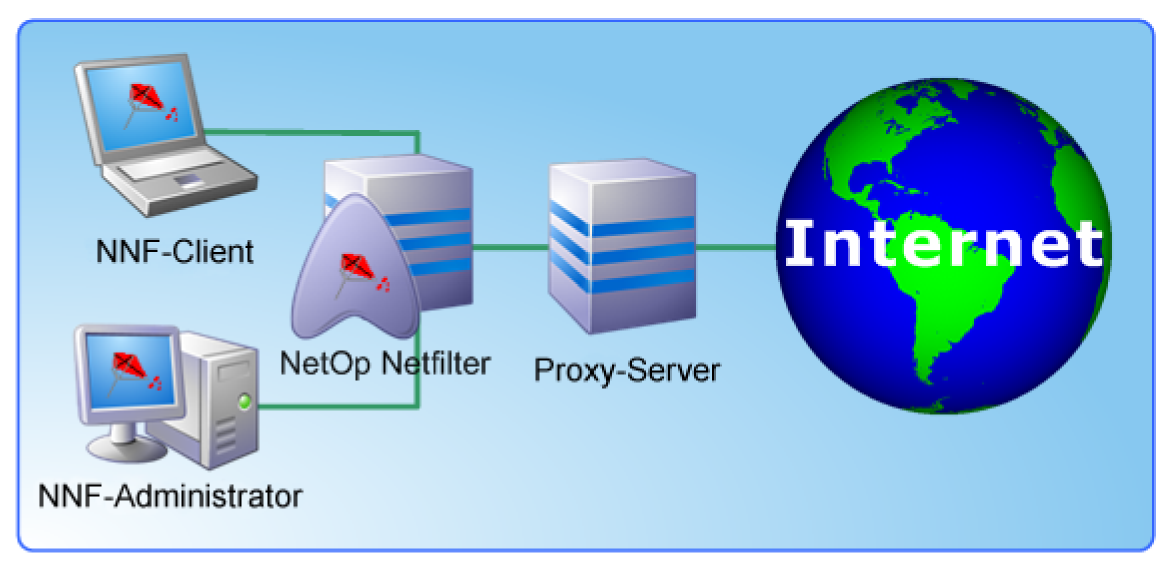


Abbildung 2: Nutzung von NetOp Netfilter mit einem externen Proxy-Server.

1.2 Kontaktinformationen

Kundenservice

Auf unserer Website finden Sie Angaben zum technischen Support sowie Antworten auf häufig gestellte Fragen:

http://www.netop.com/support

Kontaktinformationen

Adresse:

Danware Data A/S

Bregnerodvej 127

3460 Birkerod

Dänemark

E-Mail-Adresse: info@netop.com

Website: http://www.netop.com

2 Installation und Deinstallation

Die Installation von NetOp Netfilter umfasst zwei Schritte. Zunächst muss NetOp Netfilter auf einem Server mit Internet-Zugang installiert werden. Anschließend müssen die Clients, deren Internet-Datenverkehr gefiltert werden soll, so konfiguriert werden, dass diese NetOp Netfilter als Proxy-Server verwenden.

Systemvoraussetzungen

Installation auf Server

Installation auf Client-Computern

Deinstallation von NetOp Netfilter

Automatische Updates

Taskleistensymbol ausblenden

2.1 Systemvoraussetzungen

Server

Mindestanforderungen:

- Pentium-kompatibler Prozessor mit 700 MHz
- 128 MB RAM
- 50 MB freier Speicherplatz auf der Festplatte
- Microsoft Windows NT 4, Windows Server 2000/2003 (alle Server-Editionen)

Das Benutzerverhalten ist maßgebend für die Anforderungen an den Server. Handelt es sich um "durchschnittliche Benutzer", die hauptsächlich Seiten ohne pornografische Inhalte besuchen und selten große Dateien herunterladen, kann die Anzahl der von ihnen zu Spitzenzeiten erzeugten Treffer pro Sekunde verwendet werden, um die Anforderungen an die Server-Hardware einzuschätzen (mit Hilfe von Abbildung 3).

Ist die Anzahl der Treffer pro Sekunde bekannt (beispielsweise, weil bereits ein Proxy verwendet wird), lassen sich mit diesem Wert die Anforderungen an den Netfilter-Server ermitteln.

Ist die Anzahl nicht bekannt, können Sie davon ausgehen, dass ein durchschnittlicher Benutzer beim Zugriff auf das Internet einen Treffer pro Sekunde erzeugt. Wird zu Spitzenzeiten beispielsweise von 100 Computern gleichzeitig auf das Internet zugegriffen, werden 100 Treffer pro Sekunde erzeugt.

Ein Treffer pro Sekunde gilt als Durchschnittswert für eine ganze Sitzung. In sog. "Burst-Phasen" können für ein bis zwei Sekunden auch mehr als 50 Treffer pro Benutzer auftreten. Der Server muss diese Auslastung unterstützen, damit für die einzelnen Benutzer keine allzu große Verzögerung entsteht.

Prozessor (MHz)	Treffer/s.	Durchsatz (Mbit/s)
700	80	4
1333	120	6
2200	160	8

Abbildung 3: Leistung bei verschiedenen Prozessorgeschwindigkeiten. Da die Hardwareanforderungen vom Benutzerverhalten abhängen, sollten diese Werte nur als Richtlinie angesehen werden.

Hinweis: Abbildung 3 basiert auf der Annahme von 0 % Cache-Treffern. Tatsächlich bewegt sich die Anzahl der Cache-Treffer typischerweise im Bereich von 10-50 %. Aus diesem Grund kann ein Server mit einem bestimmten Prozessor eine höhere Auslastung unterstützen, als in der Tabelle angegeben.

Übersteigt die Netzwerkauslastung den Grenzwert eines einzelnen Servers, müssen mehrere Server bereitgestellt werden. Die Clients im Netzwerk müssen in diesem Fall für verschiedene Proxy-Server konfiguriert werden, so dass der Datenverkehr auf mehrere Server verteilt werden kann.

Da die Internet-Verbindung die für die Benutzer verfügbare Bandbreite begrenzt, können die Anforderungen an den Server auch anhand der Geschwindigkeit der Internet-Verbindung ermittelt werden. Vergleichen Sie dazu diesen Wert mit der Spalte *Durchsatz* in Abbildung 3.

Beachten Sie, dass der Filter zu einer Verzögerung führt. Um diese Verzögerung für die einzelnen Benutzer in angemessenen Grenzen zu halten, wird ein Server mit mindestens 700 MHz empfohlen.

Clients

Prinzipiell werden alle Browser unterstützt, die einen HTTP-Proxy verwenden können. Die im Lieferumfang enthaltene Client-Konfigurationssoftware kann die folgenden Browser automatisch konfigurieren:

- Microsoft Internet Explorer 4 und höher
- Netscape Navigator und Communicator 4
- Netscape 6 und höher sowie Mozilla
- Opera 5 und höher

Die Client-Konfigurationssoftware unterstützt:

Microsoft Windows 98, ME, NT 4, 2000, XP und Vista

Linux

Mac OS

2.2 Installation auf Server

Installation

Klicken Sie zum Installieren des Programms auf den von Danware bereitgestellten Link.

Wählen Sie entweder *Ausführen* oder *Speichern*.

Bei Auswahl von *Ausführen* wird die Installation umgehend gestartet. Bei Auswahl von *Speichern* müssen Sie die Installationsdatei manuell aktivieren, um die Installation zu starten.

Das Installationsprogramm leitet Sie durch die zur Installation von NetOp Netfilter erforderlichen Schritte. Nach Abschluss der Installation ist NetOp Netfilter als Dienst installiert und wird automatisch gestartet.

Der Standard-TCP-Port, den NetOp Netfilter für die Browser-Kommunikation verwendet, lautet 3128. Wird ein anderer Port benötigt, beispielsweise falls Port 3128 bereits von einem anderen Dienst auf dem Computer verwendet wird, kann dieser einfach mit dem im Abschnitt Netfilter-Proxy beschriebenen Programm NetOp Netfilter Admin geändert werden.

Erste Ausführung

Bevor die Clients im Netzwerk für die Verwendung von NetOp Netfilter konfiguriert werden, muss überprüft werden, ob NetOp Netfilter korrekt installiert ist und auf das Internet zugreifen kann. Wenn der Port für die Browser-Kommunikation nicht geändert wurde und Internet Explorer auf dem Computer installiert ist, kann dies mit der Anwendung NetOp Netfilter Test einfach überprüft werden (siehe Abbildung 4). Starten Sie die Anwendung, und öffnen Sie anschließend den Internet Explorer, indem Sie auf die Schaltfläche *Internet Explorer starten*

klicken. Wenn NetOp Netfilter korrekt konfiguriert ist, wird vom Browser eine Meldung angezeigt, dass NetOp Netfilter korrekt installiert wurde. Rufen Sie eine Internet-Seite auf, um die Verbindung zum Internet zu überprüfen.



Abbildung 4: Testen von NetOp Netfilter.

Sie können alternativ auch einen Browser öffnen und den Proxy-Server auf die IP-Adresse/den Namen des Computers einstellen, auf dem NetOp Netfilter installiert ist, und die Port-Nummer auf 3128 setzen (wenn in NetOp Netfilter Admin kein anderer Port ausgewählt wurde). Wenn sich der verwendete Browser auf dem gleichen Computer wie NetOp Netfilter befindet, können Sie *localhost* als Computernamen eingeben. Wählen Sie in deutschen Versionen von Internet Explorer 5 oder höher das folgende Menü aus:

```
Extras > Internetoptionen > Verbindungen > LAN-Einstellungen
```

Aktivieren Sie das Kontrollkästchen Proxy-Server verwenden. Geben Sie die IP-Adresse/den Computernamen von NetOp Netfilter im Adressfeld und 3128 im Port-Feld ein (siehe Abbildung 5). Wird der Browser auf demselben Computer wie NetOp Netfilter geöffnet, geben Sie *localhost* als Adresse ein. Das Kontrollkästchen *Proxyserver für lokale Adressen umgehen* muss deaktiviert sein.

Geben Sie im Adressfeld des Browsers die folgende Adresse ein, um zu prüfen, ob NetOp Netfilter korrekt installiert und konfiguriert ist:

```
http://are-you-alive
```

Wenn das Programm korrekt konfiguriert wurde, wird die Meldung angezeigt, dass NetOp Netfilter ordnungsgemäß installiert ist. Sie können auch eine Internet-Seite aufrufen, um sicherzustellen, dass der Server korrekt mit dem Internet verbunden ist.

Wird eine Seite nicht korrekt angezeigt, muss überprüft werden, ob diese Seite ohne NetOp Netfilter und in einem Browser, der für die Verwendung von NetOp Netfilter nicht konfiguriert ist, angezeigt werden kann. Diese Maßnahme sollte ergriffen werden, um sicherzustellen, dass

die Internet-Seite nicht vorübergehend offline ist.

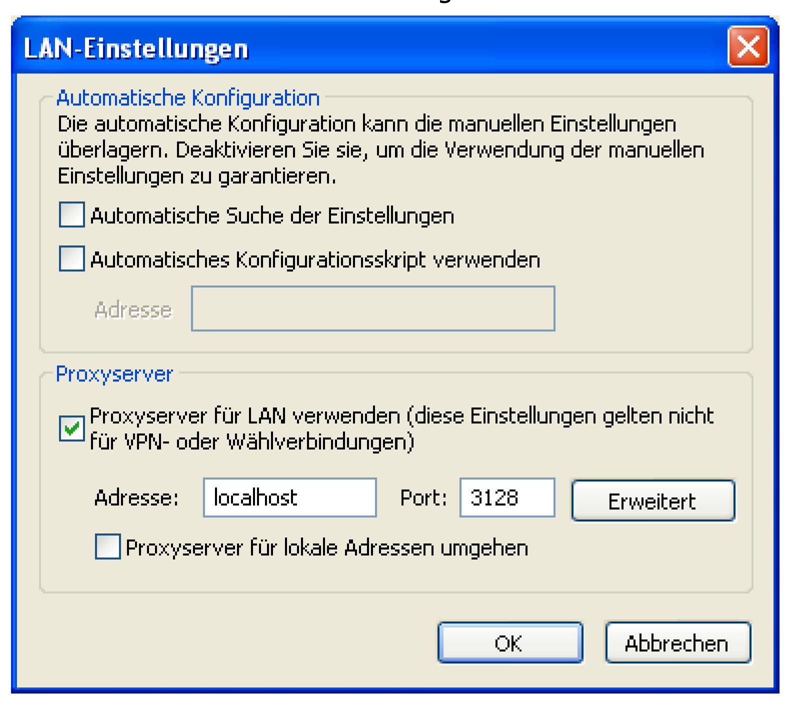


Abbildung 5: Proxy-Konfiguration.

Siehe hierzu: Server-Voraussetzungen.

2.3 Installation auf Client-Computern

Die Filterfunktion wird aktiviert, indem Sie die Web-Browser so konfigurieren, dass der Server mit NetOp Netfilter als Proxy-Server für den HTTP-Datenverkehr verwendet wird. Ist auf den Client-Computern Microsoft Windows 98, ME, NT 4, 2000, XP oder Vista installiert, können Sie hierzu die Anwendung ECLIENT oder das Konfigurations-Tool verwenden. Mit diesen Programmen können Sie außerdem Einschränkungen der Benutzerschnittstelle festlegen, die Benutzer daran hindern, Ihre Einstellungen zu ändern.

Wenn Sie in Ihrem Netzwerk die automatische Proxy-Konfiguration verwenden, können Sie zur Aktivierung des Filters im Konfigurationsskript ganz einfach die Proxy-Adresse und den Port ändern. Wenn Ihnen Tools zur Remote-Verwaltung der Browser-Einstellungen zur Verfügung stehen (beispielsweise Richtlinien oder Netscape Mission Control Desktop), können Sie auch diese verwenden.

Wenn Sie in Ihrem Netzwerk bereits einen Proxy konfiguriert haben und keine automatische Proxy-Konfiguration verwenden (und dies auch nicht beabsichtigen), können Sie den Filter auch aktivieren, indem Sie NetOp Netfilter so konfigurieren, dass die Anwendung die gleiche Adresse und den gleichen Port wie der bisher verwendete Proxy nutzt. Verlagern Sie den vorhandenen Proxy in diesem Fall auf einen anderen Port/eine andere Adresse, sofern dieser weiterhin verwendet werden soll. Auf diese Weise müssen Sie die Einstellungen der Client-Computer nicht ändern.

Siehe hierzu: Client-Voraussetzungen, ECLIENT.EXE, Konfigurations-Tool, Minimalinstallation, Vollinstallation, Clients über Active Directory verteilen und Taskleistensymbol ausblenden

2.3.1 ECLIENT.EXE

ECLIENT.EXE kann zur Änderung der Proxy-Einstellungen für Internet Explorer verwendet werden. Dieses Tool dient in einem Anmeldeskript als Alternative zu einer .reg-Datei des *Konfigurations-Tools*. ECLIENT.EXE unterstützt Windows 98, ME, NT, 2000, XP und Vista.

Darüber hinaus muss ECLIENT.EXE auf den Clients ausgeführt werden, damit die

Protokollierung von Benutzernamen, Peer-2-Peer-Sperrung und Chat-Sperrung genutzt werden kann. Werden diese Funktionen nicht benötigt, muss ECLIENT.EXE nicht auf den Clients ausgeführt werden.

Hinweis: Ist die Protokollierung der Benutzernamen aktiviert, muss ECLIENT.EXE auf allen Clients ausgeführt werden, oder ECLIENT.EXE muss mit dem Parameter /sharedip ausgeführt werden und die Unterstützung für gemeinsam genutzte IP-Adressen muss in Netfilter Admin aktiviert sein, da der Internet-Zugriff ansonsten für Clients ohne ECLIENT.EXE erheblich verlangsamt wird. Aktivieren Sie die Protokollierung der Benutzernamen erst dann, wenn ECLIENT.EXE auf allen Clients ausgeführt wird.

Wenn Sie ein heterogenes Netzwerk verwenden, in dem beispielsweise Windows 95-, 98-, XP- und Macintosh-Computer vorhanden sind, steht die Protokollierung der Benutzernamen dennoch für die unterstützten Systeme zur Verfügung. Verwenden Sie jedoch unbedingt den Parameter /sharedip. Auf diese Weise wird der Internet-Zugriff für Clients ohne ECLIENT.EXE nicht verlangsamt.

ECLIENT.EXE kann in Verbindung mit den folgenden Parametern verwendet werden:

/unamehost=addr	Name oder IP-Adresse des Servers, der für die Namensprotokollierung verwendet wird. Ist Netfilter nur auf einem Server installiert, muss hier dessen Adresse angegeben werden. Werden die Benutzernamen nicht protokolliert, kann dieser Parameter weggelassen werden.
/blockhost=addr	Name oder IP-Adresse des Servers, von dem die Einstellungen für Chat- und Peer-2-Peer-Sperrung abgerufen werden müssen. Ist Netfilter nur auf einem Server installiert, muss hier dessen Adresse angegeben werden. Sie können diesen Parameter weglassen, wenn Sie keine Chat- und Peer-2-Peer-Sperrung verwenden.
/proxyhost=addr	Name oder IP-Adresse des für die Filterung verwendeten Servers. Ist Netfilter nur auf einem Server installiert, muss hier dessen Adresse angegeben werden. Wird dieser Parameter nicht angegeben, ändert ECLIENT.EXE die Proxy-Einstellungen nicht.
/proxyport=nnnn	Port-Nummer für den Filter-Port von Netfilter. Wird dieser Parameter nicht angegeben, wird die Netfilter-Standardeinstellung 3128 verwendet.
/script=url	Adresse des Proxy-Skripts. Verwenden Sie diesen Parameter, wenn die Proxy-Einstellungen per Skript gesteuert werden.
/autodetect	Automatische Proxy-Erkennung.
/bypass=list	Liste der Adressen, für die Netfilter nicht verwendet werden soll. Der Datenverkehr an diese Adressen wird nicht durch Netfilter geleitet. Daher müssen diese Clients direkt auf die angegebenen Adressen zugreifen können. Die Adressen in dieser Liste werden durch Semikola (;) getrennt.
/local	Verwenden Sie diesen Parameter, wenn Netfilter auch als Proxy für Datenverkehr an Adressen im lokalen Netzwerk genutzt werden muss.
/disableproxy	Geben Sie diesen Parameter an, um den Proxy zu deaktivieren (beispielsweise bei der Deinstallation).
/nolock	Bei Angabe dieses Parameters wird die Benutzerschnittstelle zur Änderung der Proxy-Einstellungen nicht gesperrt, so dass der Benutzer diese Einstellungen ändern kann (sofern die Benutzerschnittstelle nicht auf andere Art und Weise gesperrt wurde).
/unlock	Legen Sie diesen Parameter fest, um die Sperre der Benutzerschnittstelle aufzuheben. Wird bei der Deinstallation verwendet.

/sharedip	Muss angegeben werden, wenn verschiedene Benutzer die gleiche IP-Adresse verwenden. Dies ist dann der Fall, wenn Citrix oder Terminal Services verwendet werden oder wenn zwischen den Benutzern und NetOp Netfilter ein weiterer Proxy-Server installiert ist. Wird der Parameter /sharedip in diesen Fällen nicht angegeben, wird der Datenverkehr nicht korrekt protokolliert. Die Protokollierung der Benutzernamen und die Unterstützung für gemeinsam genutzte IP-Adressen müssen aktiviert sein. Siehe hierzu die Beschreibung im Abschnitt Protokoll-Setup. **Hinweis:** Der Datenverkehr wird bei Verwendung des Parameters /sharedip nur dann korrekt protokolliert, wenn alle Benutzer den Browser Internet Explorer verwenden.

ECLIENT.EXE kann über die Anmeldeskripts der Benutzer ausgeführt werden. Hierzu muss das Programm zunächst in ein Netzwerkverzeichnis kopiert werden, auf das alle Clients zugreifen können. ECLIENT.EXE finden Sie im Client-Ordner in dem Verzeichnis, in dem NetOp Netfilter installiert wurde. In der Regel ist dies:

```
\Programme\Danware Data\NetOp Netfilter\ Business\Client
```

Wurde ECLIENT.EXE in das entsprechende Netzwerkverzeichnis kopiert, muss das Anmeldeskript um eine Zeile ergänzt werden, die ECLIENT.EXE mit den gewünschten Parametern startet. Beispiel:

```
\\myserver\files\eclient.exe /unamehost=10.10.10.10 /
proxyhost=10.10.10.10
```

Hinweis: Der obige Text muss in einer Zeile stehen.

Das Programm wird nun immer dann gestartet, wenn sich ein Benutzer anmeldet. Hierbei werden die Proxy-Einstellungen so gewählt, dass der angegebene Server als Proxy verwendet wird.

Sind auf den Clients lokale Firewalls installiert, müssen diese so konfiguriert sein, dass ECLIENT.EXE als Server ausgeführt werden und auf das Internet zugreifen kann.

Hinweis: Die Listen mit zu sperrenden Peer-2-Peer- und Chat-Programmen müssen nach jeweils 30 Minuten aktualisiert werden. Dies bedeutet, dass bis zu 30 Minuten vergehen können, bevor die mit dem Administrationsprogramm vorgenommenen Änderungen auf allen Clients aktiv werden.

2.3.2 Konfigurations-Tool

Wenn Sie das Konfigurations-Tool zur Konfiguration der Client-Computer verwenden möchten, können Sie dieses über das Startmenü starten:

```
Start > Programme > NetOp Netfilter > Business > Konfigurations-Tool
```

Das Programm leitet Sie durch die erforderlichen Schritte zur Konfiguration der Proxy-Einstellungen und der Einschränkungen der Benutzerschnittstelle. Wie in Abbildung 6 gezeigt, können Sie zwischen Minimalinstallation mit Registrierungsskript und Vollinstallation mit Setup-Programm wählen.

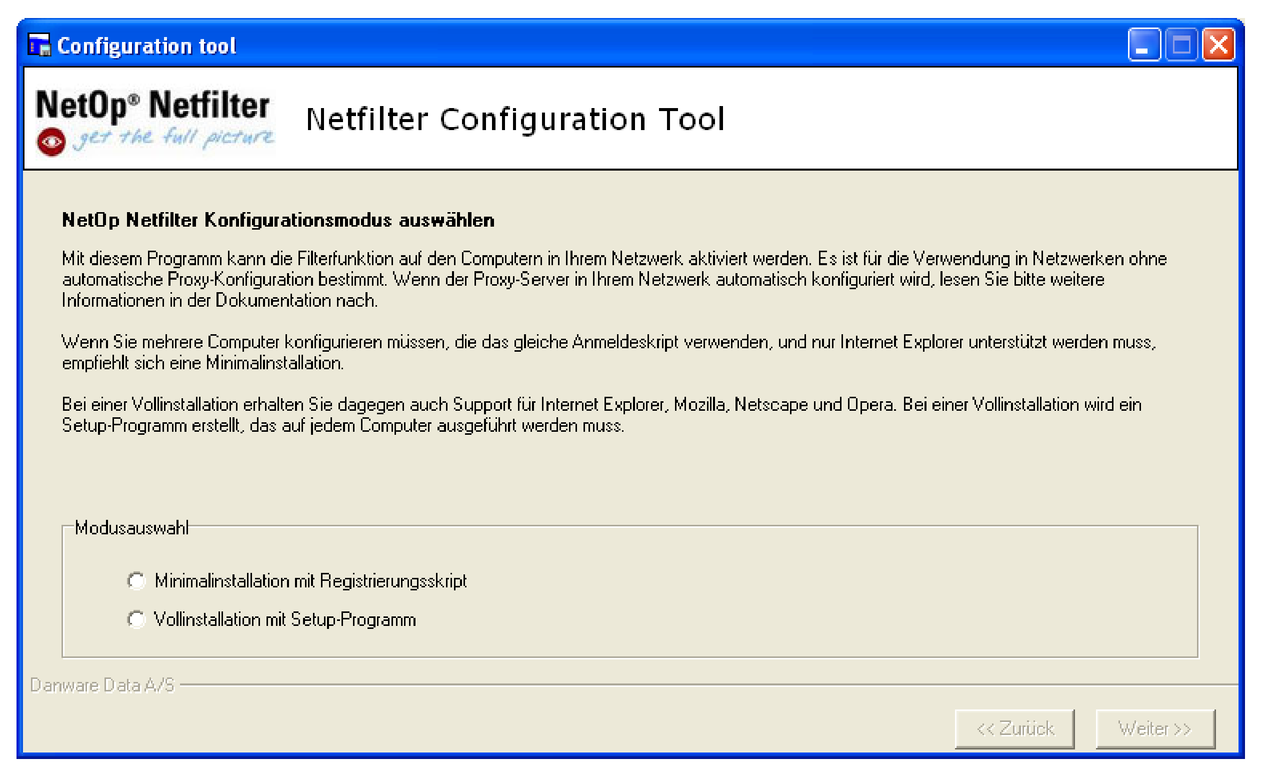


Abbildung 6: Wahl des Konfigurationsmodus.

Wählen Sie die Option Minimalinstallation aus, wenn Sie die Clients mit einer .reg-Datei für die Einstellungen von Microsoft Internet Explorer konfigurieren möchten. Wenn die Benutzer ein gemeinsames Anmeldeskript verwenden, ist die Minimalinstallation die bequemste Lösung, unterstützt jedoch nur den Internet Explorer. Bei der Minimalinstallation wird auf den Client-Computern keine Software installiert.

Wählen Sie die Option Vollinstallation, wenn Sie die Clients mit einem Setup-Programm konfigurieren möchten, das auf jedem Computer ausgeführt werden muss, für den die Filterung aktiviert werden soll. Auf den Client-Computern wird Software installiert, die bei der Anmeldung die Benutzereinstellungen korrigiert, sofern diese von den im Konfigurations-Tool gewählten Einstellungen abweichen. Diese Software konfiguriert auch Browser, die nach Abschluss der Filterinstallation installiert wurden.

Wenn Sie die Protokollierung von Benutzernamen, Peer-2-Peer-Sperrung und Chat-Sperrung verwenden möchten, muss das Programm ECLIENT.EXE auf den Client-Computern ausgeführt werden. ECLIENT.EXE kann über die Anmeldeskripts der Benutzer ausgeführt werden.

Klicken Sie nach Auswahl der gewünschten Konfiguration auf *Weiter*. Die beiden Konfigurationsarten werden in den folgenden Abschnitten ausführlich erläutert.

2.3.3 Minimalinstallation

Sie werden zunächst aufgefordert, die Adresse des Computers einzugeben, auf dem NetOp Netfilter installiert ist. Außerdem wird die von NetOp Netfilter verwendete Port-Nummer benötigt. Sofern Sie den Port in NetOp Netfilter Admin nicht geändert haben, lautet dieser 3128. Geben Sie diese Informationen auf der in Abbildung 7 gezeigten Seite ein. Sie können auch festlegen, ob die Kommunikation mit lokalen Adressen (andere Systeme im Intranet) von NetOp Netfilter gefiltert werden soll. Außerdem können Sie eine Liste von Servern einrichten, für deren Datenverkehr keine Filterung erforderlich ist (beispielsweise Ihr eigener Web-Server).

Die Option "Netfilter für Hotmail-Adressen umgehen" muss ausgewählt sein, damit der Zugriff

auf Hotmail von Outlook aus möglich ist. Ist diese Option ausgewählt, wird der Datenverkehr an Adressen, die die Zeichenfolge "hotmail" oder "services.msn" enthalten, nicht durch Netfilter geleitet. Auf diese Weise können die Benutzer von Outlook aus auf Hotmail zugreifen. Die betreffenden Adressen werden jedoch nicht durch den Filter analysiert bzw. gesperrt. Sie müssen Netfilter für diese Adressen nicht umgehen, wenn Sie mit einem Browser auf Hotmail zugreifen möchten.

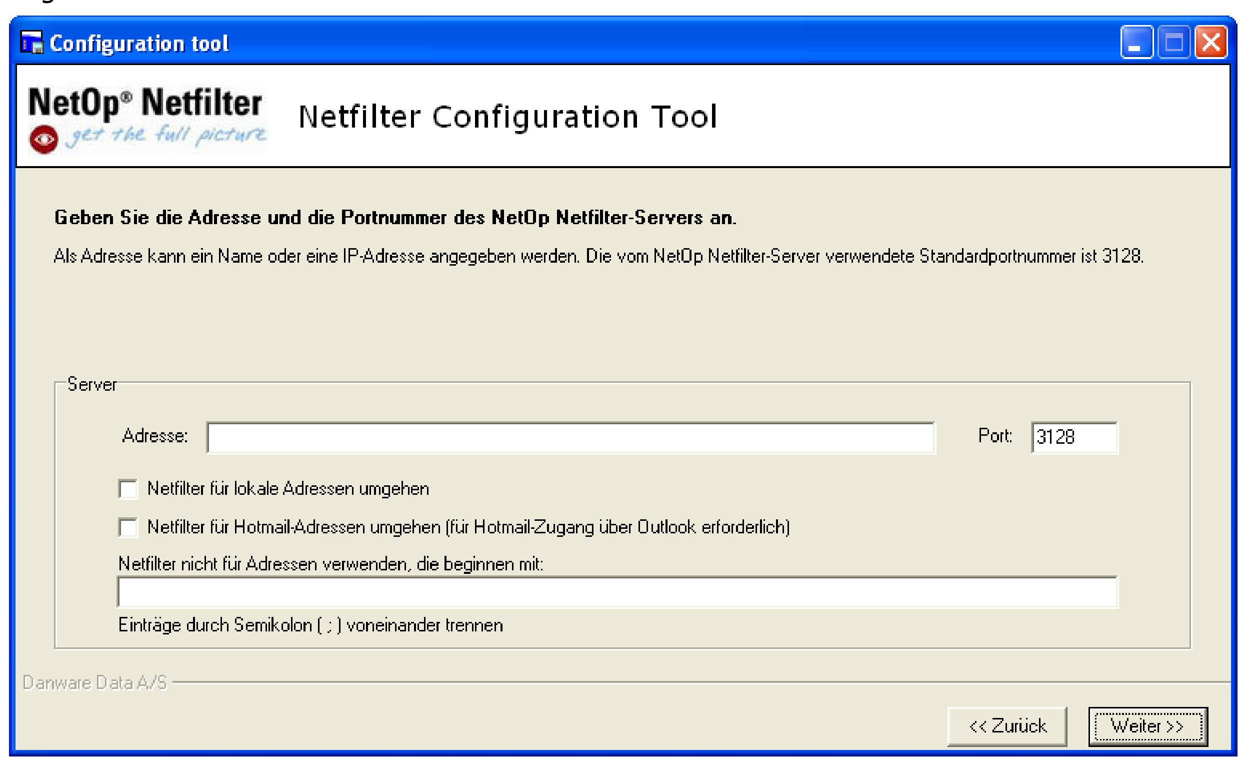


Abbildung 7: Eingabe der Proxy-Einstellungen.

Bei der Minimalinstallation können Einschränkungen der Benutzerschnittstelle nur für Client-Computer konfiguriert werden, auf denen Windows 98 oder ME installiert ist. Für Computer mit Windows NT, 2000, XP oder Vista lassen sich auf diese Weise nur die Proxy-Einstellungen definieren. Verwenden Sie die in Abbildung 8 gezeigte Seite zur Konfiguration von Einschränkungen der Benutzerschnittstelle daher nur für Clients mit Windows 98 und ME. Für diese Betriebssysteme können Sie auf dieser Seite festlegen, dass der Benutzer die Proxy-Einstellungen von Internet Explorer nicht ändern darf. Darüber hinaus können Sie auch Tools zur Änderung der Registrierung (regedit und regedt32) deaktivieren, über die die Proxy-Einstellungen für Internet Explorer ebenfalls modifiziert werden können. Unter Windows 98 und ME können sich Benutzer in der Regel auch ohne Benutzernamen anmelden, wenn sie bei der Anmeldeaufforderung die Taste ESC drücken. Dies ist bei aktivierter Protokollierung der Benutzernamen nicht wünschenswert. Wenn Sie sicherstellen möchten, dass sich die Benutzer mit einem gültigen Benutzernamen anmelden, müssen Sie die Option "Benutzer müssen sich mit gültigem Benutzernamen anmelden" aktivieren.

Der letzte Schritt bei der Minimalinstallation im Konfigurations-Tool besteht in der Erstellung einer .reg-Datei mit der gewählten Konfiguration. Auf der in Abbildung 9 gezeigten Seite müssen Sie einen Namen für die .reg-Datei eingeben. Klicken Sie anschließend auf Erstellen, um die Datei zu erstellen. Sie können das Konfigurations-Tool nun über die Schaltfläche Beenden schließen.

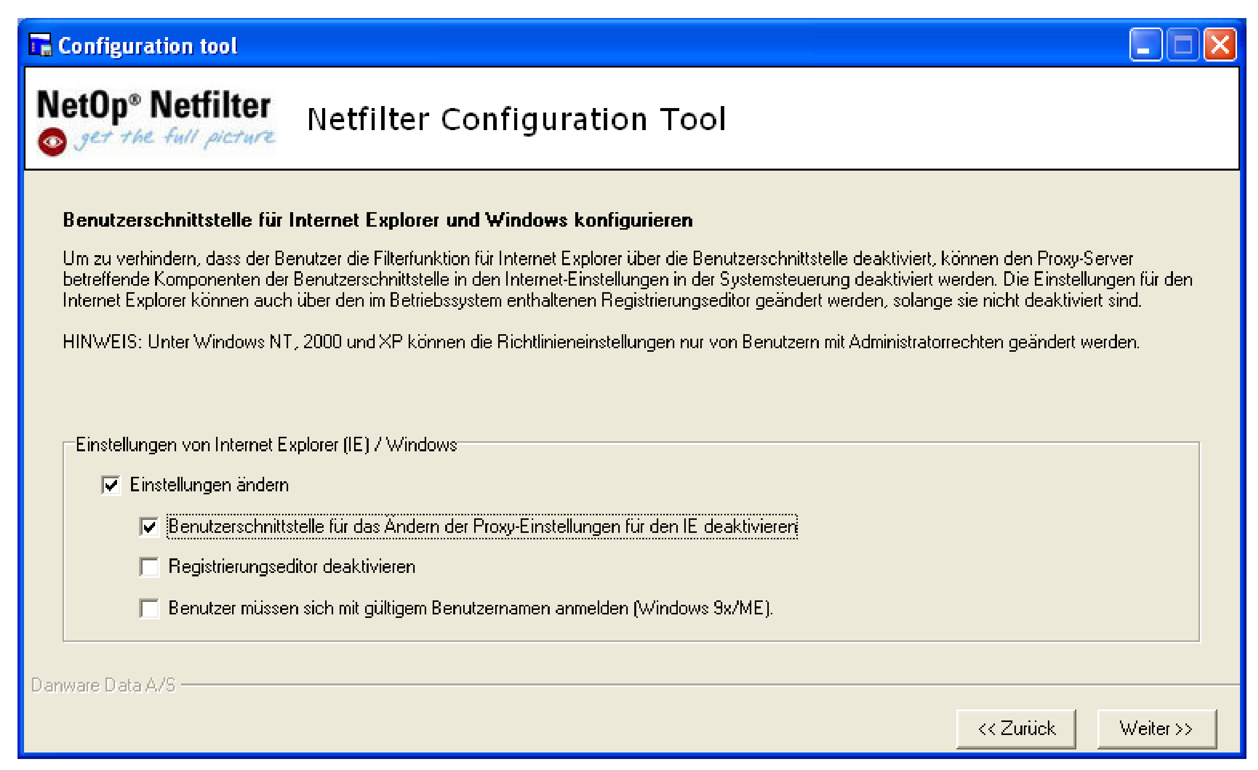


Abbildung 8: Konfigurieren der Einschränkungen für die Benutzerschnittstelle.

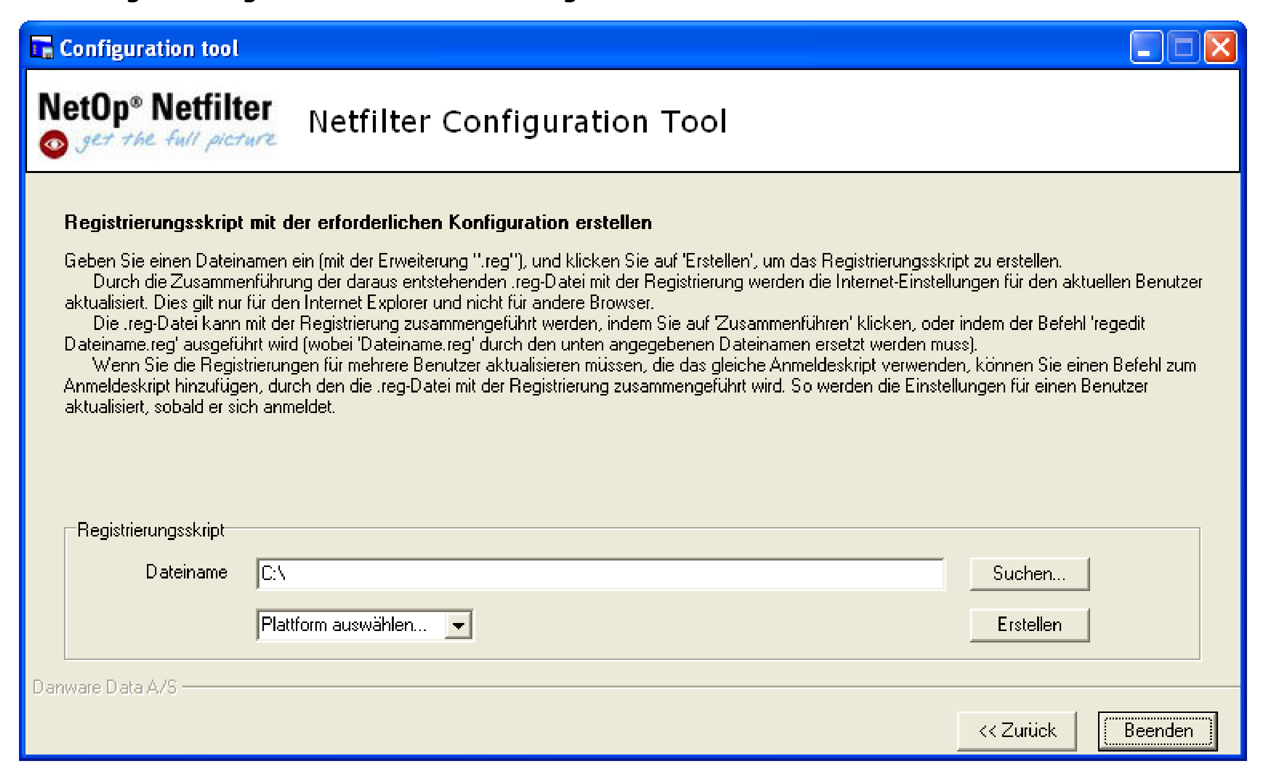


Abbildung 9: Erstellen der .reg-Datei.

Die vom Konfigurations-Tool erstellte .reg-Datei muss nun für die Aktualisierung der Einstellungen auf den Client-Computern verwendet werden.

Wenn die Benutzer ein gemeinsames Anmeldeskript verwenden, können Sie die Einstellungen vom Skript aus aktualisieren. Verwenden Sie hierzu im Anmeldeskript den folgenden Befehl:

```
regedit /s reg_Datei
```

Hierbei steht reg_Datei für den Pfad und den Namen der .reg-Datei.

Sie können die Registrierung eines Benutzers auch manuell aktualisieren, indem Sie mit der rechten Maustaste auf die .reg-Datei klicken und die Option Zusammenführen auswählen.

2.3.4 Vollinstallation

Sie werden zunächst aufgefordert, die Adresse des Computers einzugeben, auf dem NetOp Netfilter installiert ist. Außerdem wird die von NetOp Netfilter verwendete Port-Nummer benötigt. Sofern Sie den Port in NetOp Netfilter Admin nicht geändert haben, lautet dieser 3128. Geben Sie diese Informationen auf der in Abbildung 10 gezeigten Seite ein. Sie können auch festlegen, ob die Kommunikation mit lokalen Adressen (andere Systeme im Intranet) von NetOp Netfilter gefiltert werden soll. Außerdem können Sie eine Liste von Servern einrichten, für deren Datenverkehr keine Filterung erforderlich ist (beispielsweise Ihr eigener Web-Server).

Die Option "Netfilter für Hotmail-Adressen umgehen" muss ausgewählt sein, damit der Zugriff auf Hotmail von Outlook aus möglich ist. Ist diese Option ausgewählt, wird der Datenverkehr an Adressen, die die Zeichenfolge "hotmail" oder "services.msn" enthalten, nicht durch Netfilter geleitet. Auf diese Weise können die Benutzer von Outlook aus auf Hotmail zugreifen. Die betreffenden Adressen werden jedoch nicht durch den Filter analysiert bzw. gesperrt. Sie müssen Netfilter für diese Adressen nicht umgehen, wenn Sie mit einem Browser auf Hotmail zugreifen möchten.

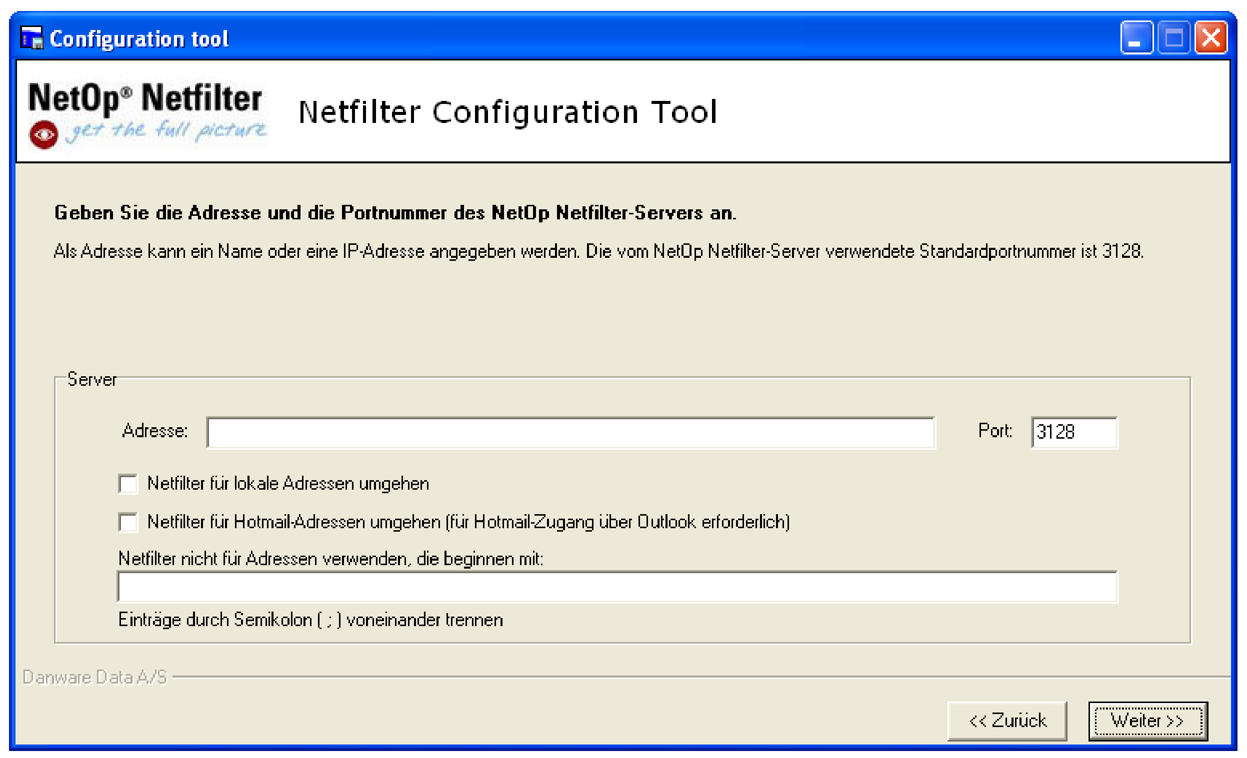


Abbildung 10: Eingabe der Proxy-Einstellungen.

Nach dem Eingeben der Proxy-Einstellungen können Sie die Einschränkungen für die Benutzerschnittstelle konfigurieren (siehe Abbildung 11). Mit diesen Einschränkungen wird es für den Benutzer schwieriger, die Proxy-Einstellungen zu ändern, um den Filter zu umgehen.

Unter Windows 98 und ME können sich Benutzer in der Regel auch ohne Benutzernamen anmelden, wenn sie während der Anmeldeaufforderung die Taste ESC drücken. Dies ist bei aktivierter Protokollierung der Benutzernamen nicht wünschenswert. Wenn Sie sicherstellen

möchten, dass sich die Benutzer mit einem gültigen Benutzernamen anmelden, müssen Sie die Option "Benutzer müssen sich mit gültigem Benutzernamen anmelden" aktivieren.

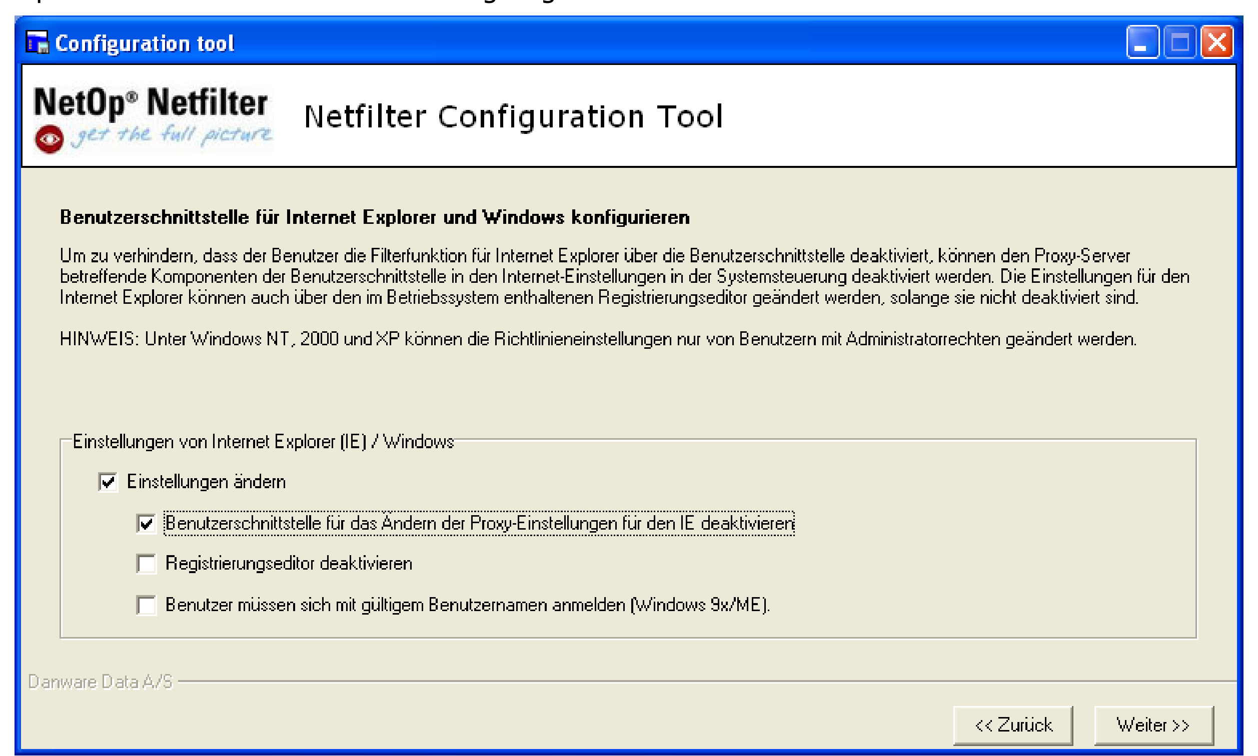


Abbildung 11: Konfigurieren der Einschränkungen für die Benutzerschnittstelle von Internet Explorer und Windows.

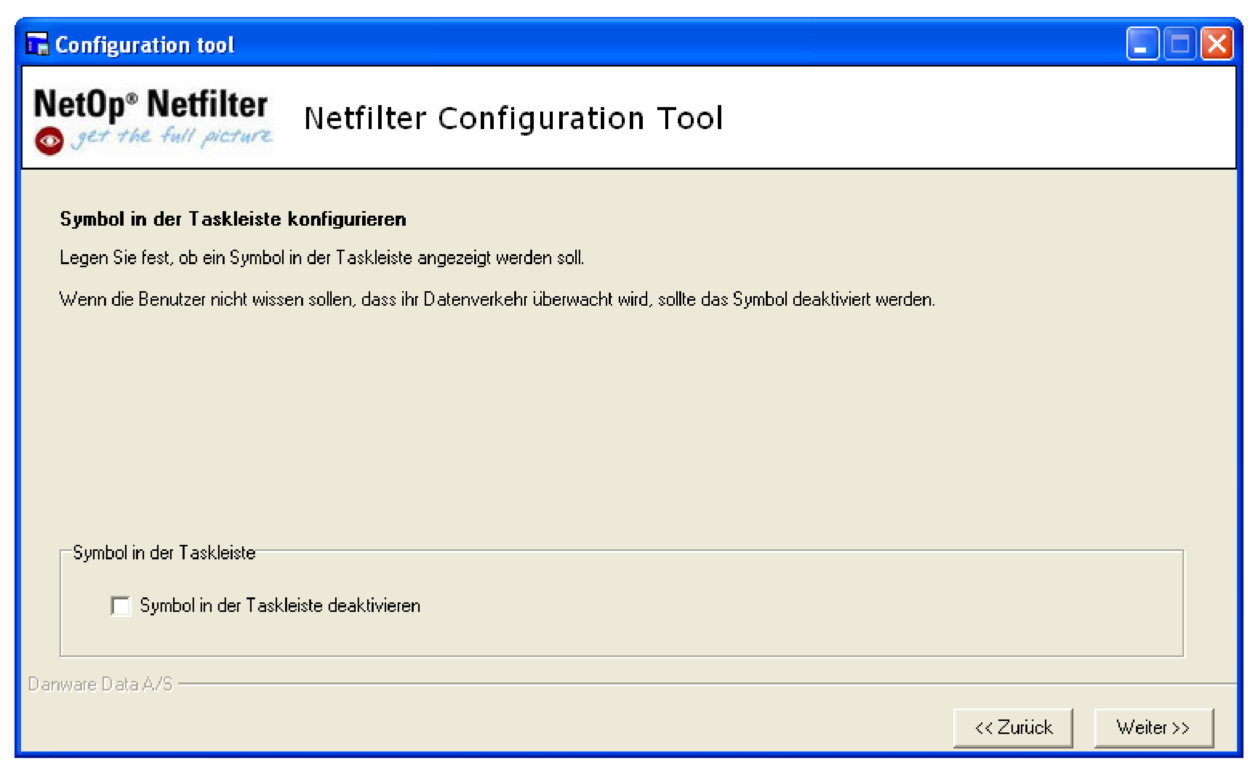


Abbildung 12: Deaktivieren des Statussymbols.

Auf der nächsten Seite (siehe Abbildung 12) können Sie das Symbol für Netfilter deaktivieren. In diesem Fall sehen die Benutzer nicht, dass ihr Internet-Datenverkehr analysiert wird.

Nach der Konfiguration der Einschränkungen kann das Programm eine Setup-Diskette erstellen. Dies erfolgt auf der in Abbildung 13 gezeigten Seite. Wählen Sie hierzu einen Pfad aus, und geben Sie die Windows-Version der Client-Systeme an.

Der Pfad für die Setup-Diskette muss nicht unbedingt auf ein Diskettenlaufwerk verweisen. Sie können auch einen anderen Speicherort auswählen (beispielsweise ein Netzlaufwerk, auf das die zu konfigurierenden Computer zugreifen können). Klicken Sie nach der Auswahl des Speicherorts auf Erstellen, um die Setup-Diskette zu erstellen. Das Konfigurations-Tool erstellt nun die erforderlichen Setup-Dateien am ausgewählten Speicherort. Zur Konfiguration eines Client-Computers muss die Datei CLISETUP.EXE auf der Setup-Diskette auf dem betreffenden Computer ausgeführt werden.

Hinweis: Unter Windows NT, 2000, XP und Vista muss CLISETUP.EXE mit Administratorrechten ausgeführt werden.

Wird CLISETUP.EXE mit dem Parameter /verysilent ausgeführt, erscheint keine Benutzerschnittstelle. Dieser Parameter kann bei automatischer Installation verwendet werden (beispielsweise in einem Anmeldeskript). Beachten Sie jedoch, dass das Programm unter den Betriebssystemen Windows NT, 2000, XP und Vista mit Administratorrechten ausgeführt werden muss. Wenn Sie sicherstellen möchten, dass CLISETUP.EXE nur einmal ausgeführt wird, können Sie prüfen, ob eine der Programmdateien bereits auf dem Computer installiert ist. Beispiel:

```
%Programme%\NetOp\Configuration Manager\ Configuration Manager.exe
```

Zur Deinstallation muss CLISETUP.EXE mit dem Parameter /uninstall ausgeführt werden. Sie können hier zusätzlich den Parameter /verysilent verwenden, um die Benutzerschnittstelle zu verbergen.

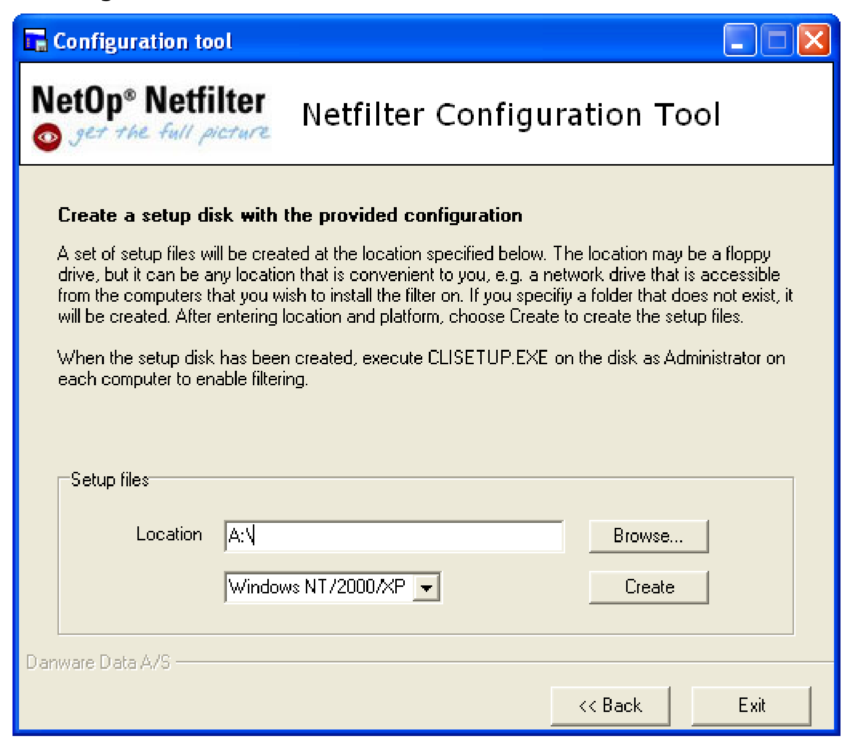


Abbildung 13: Erstellen der Setup-Diskette.

2.3.5 Clients über Active Directory verteilen

In diesem Abschnitt wird erläutert, wie NetOp Netfilter mit Hilfe von Gruppenrichtlinien für bestimmte Benutzer aktiviert wird, während gleichzeitig mit Hilfe von Active Directory für die Benutzerverwaltung anderen Benutzern ungefilterter Internet-Zugang in einer Windows-Umgebung gewährt wird.

NetOp Netfilter wird als Proxy-Server verwendet. Zur Aktivierung von Netfilter müssen die Browser eines Benutzers für die Verwendung von Netfilter als Proxy-Server beim Zugriff auf das Internet konfiguriert sein. Die folgenden Schritte beschreiben diesen Vorgang für Microsoft Internet Explorer.

Siehe hierzu: Installation auf Client-Computern, Gruppen erstellen, Benutzer einer Gruppe hinzufügen, Gruppenrichtlinie 'Netfilter Aus' konfigurieren und Fertig stellen

2.3.5.1 Gruppen erstellen

1. Öffnen Sie das Programm Active Directory-Benutzer und -Computer über das Startmenü.
2. Ermitteln Sie die Domäne mit den Benutzern, deren Internet-Verkehr gefiltert werden muss. Muss der Internet-Verkehr von Benutzern aus verschiedenen Domänen gefiltert werden, können Sie die im Folgenden beschriebenen Schritte für jede Domäne wiederholen.
3. Erstellen Sie in den gewünschten Domänen zwei Benutzergruppen: **GefilterteBenutzer** und **UngefilterteBenutzer**.
4. Sie können eine Gruppe erstellen, indem Sie mit der rechten Maustaste auf das Element klicken und dann im Kontextmenü *Neu* > *Gruppe* auswählen. Der Gruppentyp sollte Sicherheit lauten und der Bereich Lokale Domäne.

2.3.5.2 Benutzer einer Gruppe hinzufügen

1. Fügen Sie alle Benutzer, die den Netfilter-Proxy verwenden sollen, der Gruppe GefilterteBenutzer und alle anderen Benutzer der Gruppe UngefilterteBenutzer hinzu. Sie können Benutzer zu einer Gruppe hinzufügen, indem Sie
   - auf die Gruppe doppelklicken und dann auf der Registerkarte Mitglieder im Fenster der Gruppeneigenschaften die gewünschten Benutzer auswählen,
   - auf die hinzuzufügende Person doppelklicken und dann auf der Registerkarte Mitglied im Fenster der Benutzereigenschaften die Gruppe auswählen oder
   - die gewünschten Benutzer auswählen, mit der rechten Maustaste auf einen Benutzer klicken und dann die Option Mitglieder zu einer Gruppe hinzufügen auswählen.

Gruppenrichtlinie "Netfilter Ein" erstellen

2. Öffnen Sie das Fenster mit den Eigenschaften für die Domäne, indem Sie mit der rechten Maustaste auf die Domäne klicken und Eigenschaften auswählen. Gehen Sie zur Registerkarte Gruppenrichtlinie.
3. Eine Gruppenrichtlinie hinzufügen und benennen:
   - Klicken Sie auf Neu, um eine neue Gruppenrichtlinie hinzuzufügen, und nennen Sie diese **Netfilter Ein**.
   - Öffnen Sie das Fenster mit den Eigenschaften für diese Richtlinie, indem Sie auf die Schaltfläche Eigenschaften klicken. Wählen Sie in diesem Fenster die Registerkarte Sicherheit. Wählen Sie die Gruppe Authentifizierte Benutzer und entfernen Sie in der Spalte *Zulassen* das Häkchen für Gruppenrichtlinie übernehmen.
   - Klicken Sie auf *Hinzufügen*, um eine neue Gruppe hinzuzufügen. Ein neues Fenster wird geöffnet. Wählen Sie die Gruppe GefilterteBenutzer aus und klicken Sie auf *Hinzufügen* und anschließend auf *OK*.

- Aktivieren Sie auf der Registerkarte *Sicherheit* das Kontrollkästchen *Zulassen* neben *Gruppenrichtlinie übernehmen*. Klicken Sie auf *OK*.

4. Gruppenrichtlinie "Netfilter Aus" erstellen

  - Klicken Sie auf *Neu*, um eine neue Gruppenrichtlinie hinzuzufügen, und nennen Sie diese **Netfilter Aus**.
  - Öffnen Sie das Fenster mit den Eigenschaften für diese Richtlinie, indem Sie auf die Schaltfläche *Eigenschaften* klicken. Wählen Sie in diesem Fenster die *Registerkarte Sicherheit*. Wählen Sie die Gruppe *Authentifizierte Benutzer* und entfernen Sie in der *Spalte Zulassen* das Häkchen für *Gruppenrichtlinie übernehmen*.
  - Klicken Sie auf *Hinzufügen*, um eine neue Gruppe hinzuzufügen. Wählen Sie die Gruppe UngefilterteBenutzer aus und klicken Sie auf *Hinzufügen* und anschließend auf *OK*.
  - Aktivieren Sie auf der Registerkarte *Sicherheit* das Kontrollkästchen *Zulassen* für *Gruppenrichtlinie übernehmen*. Klicken Sie auf *OK*.

5. Gruppenrichtlinie "Netfilter Ein" konfigurieren

  - Doppelklicken Sie auf die Richtlinie *Netfilter Ein*. Das Snap-In der *Gruppenrichtlinie* wird geöffnet.
  - Rufen Sie *Benutzerkonfiguration > Windows-Einstellungen > Internet Explorer-Wartung > Verbindung* auf, und doppelklicken Sie auf *Proxy-Einstellungen*.
  - Aktivieren Sie das Kontrollkästchen *Proxy-Einstellungen aktivieren* und geben Sie die Adresse und die Port-Nummer des Netfilter-Proxys in die beiden HTTP-Felder ein. Deaktivieren Sie das Kontrollkästchen *Für alle Adressen denselben Proxyserver verwenden*. Wenn Sie weitere Proxys für andere Arten von Datenverkehr verwenden, müssen die Adressen und Port-Nummern der betreffenden Proxys in die übrigen Felder eingegeben werden. Legen Sie unter *Ausnahmen* beliebige Ausnahmen fest. Hinweis: Ist das Kontrollkästchen *Proxyserver nicht für lokale (Intranet-) Adressen verwenden* aktiviert, werden Websites in Ihrem Intranet nicht gefiltert. Klicken Sie auf *OK*, um zum Fenster *Gruppenrichtlinie* zurückzukehren.
  - Wenn Sie für Ihr Netzwerk die automatische Browser-Konfiguration verwenden, sollten Sie diese Funktion für die Benutzer der Gruppe GefilterteBenutzer deaktivieren. Doppelklicken Sie hierfür auf *Automatische Browser-Konfiguration* und deaktivieren Sie die Kontrollkästchen *Automatische Ermittlung von Konfigurationseinstellungen* und *Automatische Konfiguration aktivieren*.
  - Wenn Sie Benutzer daran hindern möchten, die Proxy-Einstellungen zu ändern (und dadurch den Filter zu umgehen), wählen Sie *Benutzerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Internet Explorer*.
  - Doppelklicken Sie auf *Änderung der Proxy-Einstellungen deaktivieren* und wählen Sie die Einstellung *Aktiviert*. Diese Einstellung können Sie auch für die Richtlinien *Änderung der Einstellungen für die automatische Konfiguration deaktivieren*, *Änderung der Verbindungseinstellungen deaktivieren* und/oder *Assistent für Internetzugang deaktivieren* vornehmen.
  - Wählen Sie *Benutzerkonfiguration > Administrative Vorlagen*. Klicken Sie mit der rechten Maustaste auf *Administrative Vorlagen* und wählen Sie die Option *Vorlagen hinzufügen/ entfernen*. Daraufhin wird ein neues Fenster geöffnet. Klicken Sie auf *Hinzufügen* und öffnen Sie die Datei **netfilter.adm**. Diese Datei befindet sich im Skripte-Unterverzeichnis des Installationsverzeichnisses von NetOp Netfilter. Klicken Sie auf *Schließen*, um zum Gruppenrichtlinienfenster zurückzukehren.
  - Im Gruppenrichtlinienfenster wird nun der Eintrag *Benutzerkonfiguration > Administrative Vorlagen > NetOp Netfilter* angezeigt. Klicken Sie zuerst mit der linken und dann mit der rechten Maustaste auf NetOp Netfilter und stellen Sie sicher, dass die Option *Anzeigen > Nur Richtlinien anzeigen* (*) deaktiviert ist. Doppelklicken Sie

anschließend auf die Internet Explorer-Einstellungen und aktivieren Sie die Richtlinie. Klicken Sie auf *OK*, um die Standardeinstellungen zu akzeptieren. (Die Option HTTP 1.1 über Proxyverbindungen verwenden sollte zur Erzielung der bestmöglichen Leistung aktiviert sein. Es wird prinzipiell empfohlen, für die beiden Einträge "Max. Verbindungen…" die Standardwerte zu verwenden. Durch Erhöhen der Werte können jedoch die beim Surfen über den Proxy auftretenden Verzögerungen verringert werden. Werden die Werte allerdings zu hoch gewählt, gehen Browser-Anfragen verloren und auf den aufgerufenen Websites erfolgt eine unvollständige Bildanzeige.

*) In Windows Server 2003 ist die Option Nur Richtlinien anzeigen in ein Dialogfeld verschoben worden, das Sie über Auswahl von Anzeigen > Filtern... im Menü öffnen können. Der Name der Option wurde geändert in Nur vollständig verwaltbare Richtlinieneinstellungen anzeigen.

- Schließen Sie das Snap-in der *Gruppenrichtlinie.*

2.3.5.3 Gruppenrichtlinie 'Netfilter Aus' konfigurieren

1. Doppelklicken Sie auf die Richtlinie *Netfilter Aus*. Das Snap-In der *Gruppenrichtlinie* wird geöffnet.
2. Rufen Sie *Benutzerkonfiguration > Windows-Einstellungen > Internet Explorer-Wartung > Verbindung* auf, und doppelklicken Sie auf *Proxy-Einstellungen*.
3. Sie können nun die Proxy-Einstellungen beliebig konfigurieren: Wählen Sie entweder den direkten Zugriff auf das Internet (dafür muss die Option Proxy-Einstellungen aktivieren deaktiviert sein) oder den Zugriff über einen Proxy-Server.
4. Wenn Sie für Ihr Netzwerk die automatische Browser-Konfiguration verwenden, müssen Sie diese Funktion möglicherweise für die Benutzer der Gruppe UngefilterteBenutzer aktivieren. Doppelklicken Sie hierfür auf *Automatische Browser-Konfiguration* und aktivieren Sie die Kontrollkästchen *Automatische Ermittlung von Konfigurationseinstellungen* und/oder *Automatische Konfiguration aktivieren*. Geben Sie anschließend die übrigen Informationen wie gewünscht ein.
5. Um die hier vorgenommenen Änderungen rückgängig zu machen, damit Benutzer keine Änderungen der Proxy-Einstellungen vornehmen können (wenn ein Benutzer aus der Gruppe GefilterteBenutzer in die Gruppe UngefilterteBenutzer verschoben wird), wählen Sie *Benutzerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Internet Explorer*.

Doppelklicken Sie auf *Änderung der Proxy-Einstellungen deaktivieren*, und wählen Sie die Einstellung *Deaktiviert*. Diese Einstellung können Sie auch für die Richtlinien *Änderung der Einstellungen für die automatische Konfiguration deaktivieren,* Änderung der Verbindungseinstellungen deaktivieren *und/oder* Assistent für Internetzugang deaktivieren *vornehmen.* Schließen Sie das Fenster *Gruppenrichtlinie*.

2.3.5.4 Fertig stellen

Schließen Sie das Fenster mit den Eigenschaften für die Domäne sowie das Fenster *Active Directory-Benutzer und -Computer*. Die Benutzer, die Sie zur Gruppe GefilterteBenutzer hinzugefügt haben, verwenden ab jetzt für den Zugriff auf das Internet den Netfilter-Proxy. (Möglicherweise müssen sie sich zuerst neu anmelden, damit die neue Richtlinie wirksam wird.)

Benutzer der Gruppe GefilterteBenutzer, die ungefilterten Zugriff auf das Internet benötigen, können einfach aus der Gruppe GefilterteBenutzer in die Gruppe UngefilterteBenutzer verschoben werden. Hinweis: Das Entfernen eines Benutzers aus der Gruppe GefilterteBenutzer reicht möglicherweise nicht aus, um den Netfilter-Proxy für den

betreffenden Benutzer zu deaktivieren. Der Benutzer sollte außerdem zur Gruppe UngefilterteBenutzer hinzugefügt werden, damit die Proxy-Einstellungen geändert werden. Entsprechend können Benutzer auch aus der Gruppe UngefilterteBenutzer in die Gruppe GefilterteBenutzer verschoben werden, damit die Filterfunktion für diese Benutzer aktiviert wird.

2.3.6 Business Desktop - Installation

Installieren Sie *NetOp Netfilter Business Desktop* auf mobilen PCs, die Sie mit *NetOp Netfilter* schützen möchten, auch wenn sie nicht mit dem durch *NetOp Netfilter* geschützten Netzwerk verbunden sind.

Automatische Installation

1. Erstellen Sie eine Gruppe mit dem Namen *Business Desktop*. Eine Erläuterung hierzu finden Sie unter *Gruppen erstellen*.

2. Übernehmen Sie die Gruppenrichtlinie *Netfilter Ein* für die Gruppe *Business Desktop*. Eine Beschreibung dazu finden Sie unter *Benutzer einer Gruppe hinzufügen*.

3. Aktivieren Sie die *Business Desktop-Einstellungen* in der Gruppenrichtlinie *Netfilter Ein* unter *Computer-Konfiguration > Administrative Vorlagen > NetOp Netfilter*. Geben Sie die Adresse des *NetOp Netfilter* Servers als *Adresse des Netfilter-Servers* an. *Business Desktop* kontaktiert den Server, um Einstellungen und Protokolldateien auszutauschen.

4. Kopieren Sie das Installationspaket *NetOp Netfilter Business Desktop.msi* aus dem Ordner *Programme > Danware Data > NetOp Netfilter > Business > Client* in einen Freigabeordner, auf den von den mobilen PCs zugegriffen werden kann, auf denen der Business Desktop installiert werden soll.

5. Klicken Sie in der Gruppenrichtlinie *Netfilter Ein* mit der rechten Maustaste auf *Computer-Konfiguration > Software-Einstellungen > Software-Installation*, und wählen Sie *Neu > Paket*. Wählen Sie das Installationspaket im Freigabeordner, und klicken Sie auf *Öffnen*. Wählen Sie *Erweitert*, und klicken Sie auf *OK*.

6. Wählen Sie auf der Registerkarte *Verteilung* die Option *Zugewiesen* und anschließend *Diese Anwendung bei Anmeldung installieren*. Das *Business Desktop* Paket wird nun auf den Netzwerk-Computern installiert, sobald sich die jeweiligen Benutzer anmelden.

7. Um ein Installations-Update mit einem aktualisierten Installationspaket durchzuführen, überschreiben Sie das Installationspaket im Freigabeordner. Klicken Sie in der Gruppenrichtlinie *Netfilter Ein* unter *Computer-Konfiguration > Software-Einstellungen > Software-Installation* mit der rechten Maustaste auf *NetOp Netfilter Business Desktop*, und wählen Sie *Alle Tasks > Anwendung erneut verteilen*.

Manuelle Installation

1. Ordnen Sie in der Computer-Registrierung unter dem Schlüssel *HKEY_LOCAL_MACHINE \SOFTWARE\EnoLogic\NetFilter\Business* die Server-Adresse von *NetOp Netfilter* dem Wert *ServerName* unter *REG_SZ* zu.

2. Führen Sie das Installationspaket *NetOp Netfilter Business Desktop.msi* auf dem Computer aus.

Taskleistensymbol ausblenden

Standardmäßig wird das *NetOp Netfilter* Symbol in der Taskleiste in der rechten unteren Ecke des Bildschirms angezeigt.

Um das Symbol anhand einer Gruppenrichtlinie auszublenden, doppelklicken Sie in der Gruppenrichtlinie *Netfilter Ein* unter *Computer-Konfiguration > Administrative Vorlagen > NetOp Netfilter* auf die Richtlinie *Taskleistensymbol ausblenden*, und wählen Sie *Aktivieren*. Bei der nächsten Anmeldung wird die Änderung wirksam.

2.3.7 Taskleistensymbol ausblenden

Nach der Installation des Clients wird ein Netfilter-Symbol in der Taskleiste angezeigt.

Die Deaktivierung des Symbols kann aus unterschiedlichen Gründen erfolgen und bedeutet, dass der Client im verdeckten, d. h. für den Benutzer unsichtbaren, Modus ausgeführt wird.

Warnung: In einigen Ländern müssen die Benutzer sehen können, ob sie überwacht werden. Informieren Sie sich über die örtlichen Bestimmungen und das geltende Arbeitsrecht.

Gehen Sie folgendermaßen vor, um das Taskleistensymbol in Business Desktop über Active Directory zu aktivieren:

1. Rufen Sie Computer-Konfiguration > Administrative Vorlagen > NetOp Netfilter auf.
2. Doppelklicken Sie auf *Taskleistensymbol ausblenden* und
3. ändern Sie die Option in *Aktiviert*.

Die Änderungen werden bei der nächsten Benutzeranmeldung wirksam.

Siehe hierzu: Benutzer einer Gruppe hinzufügen

2.4 Deinstallation von NetOp Netfilter

Wenn Sie NetOp Netfilter deinstallieren, aber dennoch weiterhin einen Proxy-Server verwenden möchten, können Sie die Deinstallation auf den Clients überspringen und den Proxy-Server mit der Adresse und dem Port von NetOp Netfilter zur Deinstallation verwenden. Andernfalls wird empfohlen, das Programm zunächst auf den Clients zu deinstallieren, da bis zur erfolgten Deinstallation von diesen Computern kein HTTP-Zugriff auf das Internet möglich ist.

Hinweis: Über den Bereich Software in der Windows Systemsteuerung können Sie außerdem NNF Business Administration reparieren. Die wichtigste Funktion dabei ist die Möglichkeit, Benutzernamen und Kennwort zurückzusetzen.

2.4.1 NetOp Netfilter von Client-Computern deinstallieren

Die Deinstallation von NetOp Netfilter variiert je nachdem, ob Sie die Minimal- oder Vollinstallation verwendet haben. Die hier enthaltenen Informationen gelten nur für den Fall, dass Sie das Konfigurations-Tool zur Installation verwendet haben.

2.4.2 ECLIENT.EXE deinstallieren

Werden die Proxy-Einstellungen mit ECLIENT.EXE definiert, wird das Anmeldeskript wie folgt geändert:

```
\\myserver\files\eclient.exe /disableproxy /unlock
```

Auf diese Weise wird die Proxy-Verwendung deaktiviert, und die Benutzerschnittstelle wird freigegeben. Sobald sich alle Benutzer angemeldet haben, kann diese Zeile aus dem Anmeldeskript entfernt werden. Wenn Sie den Parameter /nolock verwendet haben, können Sie den Parameter /unlock in der obigen Zeile weglassen.

2.4.3 Minimalinstallation deinstallieren

Wenn Sie eine Minimalinstallation durchgeführt haben, kann der Filter für die Client-Computer mit Hilfe einer .reg-Datei deaktiviert werden, die die ursprünglichen Einstellungen wiederherstellt. Handelt es sich bei den ursprünglichen Einstellungen um die Standardeinstellungen für Windows/Internet Explorer, können Sie die Datei NETFILTER_9X_OFF.REG oder NETFILTER_NT_OFF.REG verwenden. Diese Dateien befinden sich im Skriptordner im Installationsverzeichnis von NetOp Netfilter, in der Regel befindet sich

dies unter*Program Files\Danware Data\NetOp Netfilter\Business*. Bei Client-Computern mit Windows 98 oder ME müssen Sie die Datei NETFILTER_9X_OFF.REG verwenden. Die Datei NETFILTER_NT_OFF.REG ist für Client-Computer mit Windows NT, 2000, XP oder Vista vorgesehen.

2.4.4 Vollinstallation deinstallieren

Die Client-Software wird durch Starten von CLISETUP.EXE von der Setup-Diskette mit dem Parameter /uninstall deinstalliert. Siehe hierzu auch den Abschnitt Vollinstallation. Möglicherweise müssen Sie den Computer neu starten, um die Deinstallation abzuschließen. Der Neustart erfolgt jedoch nicht automatisch, und Sie werden auch nicht durch eine Meldung darauf hingewiesen.

Nach der Deinstallation wird der Datenverkehr dieses Clients nicht mehr gefiltert.

2.4.5 Server deinstallieren

Die Server-Software wird mit Hilfe der Funktion Software in der Systemsteuerung deinstalliert. Gehen Sie folgendermaßen vor:

- Öffnen Sie die Systemsteuerung.
- Öffnen Sie Software, und wählen Sie den Eintrag NetOp Netfilter.
- Klicken Sie auf *Entfernen*.

NetOp Netfilter wird nun deinstalliert.

2.5 Automatische Updates mit NetUpdate

Mit NetUpdate können Sie das installierte NetOp-Produkt über das Internet aktualisieren. Starten Sie das Programm über die Taskleiste von NetOp Netfilter oder über das Startmenü.

Wenn Sie Windows NT, 2000, XP oder Vista verwenden, müssen Sie zum Zeitpunkt der Programmausführung als Administrator angemeldet sein, da Sie andernfalls keine Aktualisierungen durchführen können.

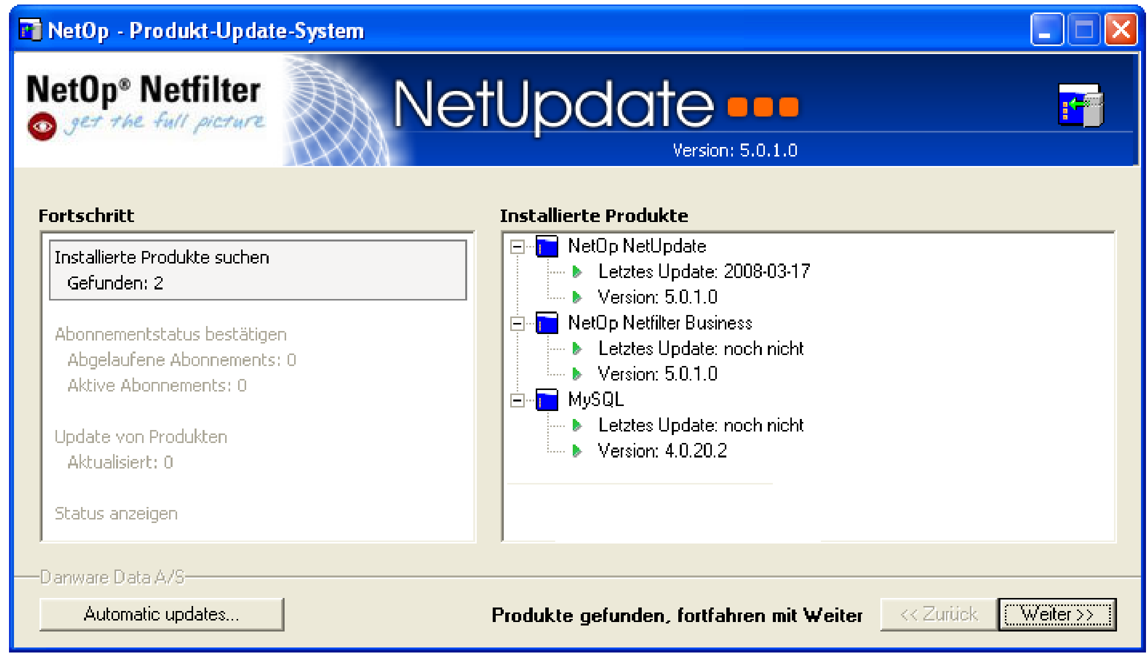


Abbildung 44: NetUpdate.

3 Konfiguration und Überwachung des Servers

Die Einstellungen für NetOp Netfilter können mit dem Programm NetOp Netfilter Admin geändert werden. Mit diesem Programm können Sie auch Statistiken zum Datenverkehr anzeigen, der durch den Filter geleitet wird. NetOp Netfilter Admin kann über das Startmenü gestartet werden:

```
Start > Programme > NetOp Netfilter > Business > Netfilter Admin
```

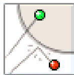
NetOp Netfilter Admin kann lokal auf einem Filter-Server (Server, auf dem NetOp Netfilter installiert ist) ausgeführt werden. Auch die Remote-Verwaltung über einen anderen Computer im Netzwerk ist möglich, wenn NetOp Netfilter Admin auf diesem Computer gestartet wird. Bei der Remote-Verwaltung muss die IP-Adresse des zu verwaltenden Filter-Servers bekannt sein.

Anmeldung

Navigation in NetOp Netfilter Admin

Fehlerbehebung

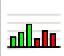
Filter



Erweitert



Statistik



Die Option Proxy



3.1 Anmeldung

Wenn NetOp Netfilter Admin gestartet wird, erscheint das in Abbildung 14 gezeigte Anmeldefenster. In diesem Fenster müssen die IP-Adresse des Filter-Servers und die Nummer des Administrations-Ports für NetOp Netfilter angegeben werden.

Wurde NetOp Netfilter Admin auf dem Filter-Server gestartet, kann die IP-Adresse 127.0.0.1, die auf *localhost* (dem Computer, auf dem NetOp Netfilter Admin gestartet wurde) verweist, unverändert bleiben. Andernfalls müssen Sie die IP-Adresse des zu verwaltenden Filter-Servers eingeben. Die Port-Nummer 9600 kann unverändert bleiben, sofern NetOp Netfilter nicht manuell für einen anderen Port konfiguriert wurde. Sollte dies der Fall sein, muss die geänderte Port-Nummer eingetragen werden. Die Änderung des Administrations-Ports wird im Abschnitt Netfilter-Proxy beschrieben.

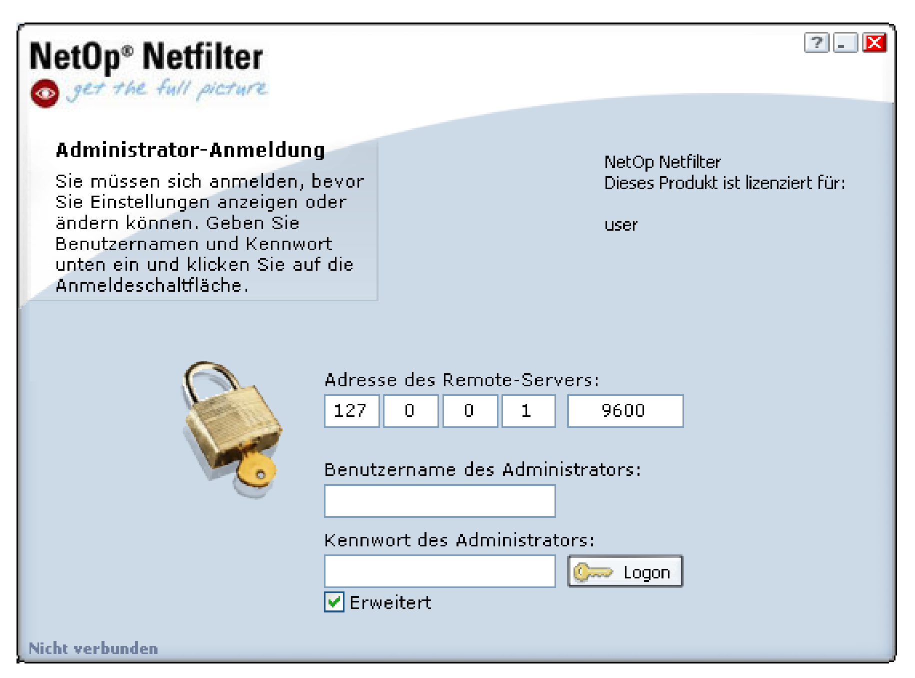


Abbildung 14: Anmeldung am Filter-Server.

Zur Erhöhung der Sicherheit ist es erforderlich, sich mit Benutzernamen und Kennwort am Filter-Server anzumelden, bevor die Verwaltungsfunktionen genutzt werden können. Wird NetOp Netfilter Admin zum ersten Mal gestartet, lauten Benutzername und Kennwort "admin".

Wenn Sie den Benutzernamen und das Kennwort eingegeben haben, klicken Sie auf die Schaltfläche Anmelden. Nach erfolgter Anmeldung am Filter-Server erscheint das in Abbildung 15 gezeigte Fenster. War die Anmeldung nicht erfolgreich, erscheint eine Fehlermeldung.

Siehe hierzu: Fehlerbehebung

3.2 Navigation in NetOp Netfilter Admin

Nach der erfolgreichen Anmeldung erscheint die in Abbildung 15 gezeigte Startseite. Hier finden Sie allgemeine Informationen zur Version sowie Statistiken. Wenn Sie eine der vier Optionen im rechten oberen Bereich des Fensters auswählen, können Sie in NetOp Netfilter Admin navigieren. Nach der Anmeldung ist die Option Filter aktiv. Einige Optionen sind weiter unterteilt. Sie können auf die untergeordneten Elemente zugreifen, indem Sie auf eine der Registerkarten am unteren Fensterrand klicken. Der Name der ersten Registerkarte der Option Filter lautet Status.

Siehe hierzu: Fehlerbehebung

3.3 Filter

Unter Filter finden Sie Informationen und Optionen für die Standardkonfiguration von NetOp Netfilter. Die verschiedenen Registerkarten für Filter werden in den folgenden Abschnitten beschrieben.

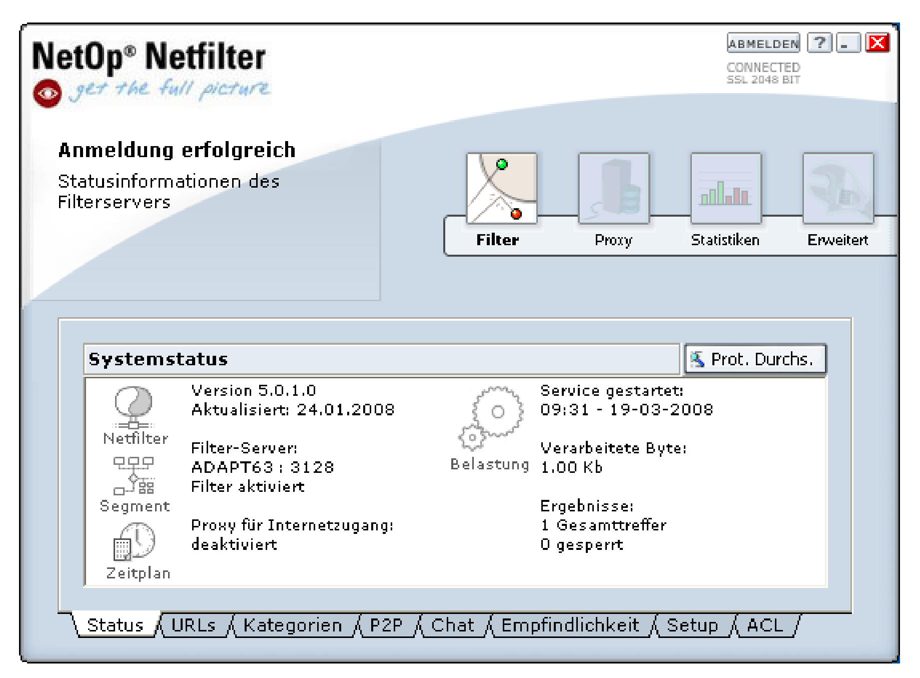


Abbildung 15: Statusseite nach dem Anmelden.

Siehe hierzu: Fehlerbehebung

3.3.1 Status

Über die Registerkarte Status können Sie Informationen zu NetOp Netfilter anzeigen. Wie Abbildung 15 zeigt, können folgende Informationen angezeigt werden:

- Die Versionsnummer von NetOp Netfilter,
- auf welchen Computern und Ports der Filter ausgeführt wird,
- ob der Filter aktiviert ist und
- ob der Filter einen Internet-Proxy verwendet.

Außerdem erhalten Sie Einblick in die Filterstatistik. Hierzu zählen Informationen zum Startzeitpunkt des Filters, zur gefilterten Datenmenge in Byte, zur Anzahl der gefilterten Seiten sowie zur der Anzahl gesperrten Seiten.

Über die Schaltfläche *Protokoll durchsuchen* können Sie sämtliche Statistiken im Detail anschauen. Ein Browser mit einer Statistikseite wird geöffnet, die Informationen zum freigegebenen und gesperrten Datenverkehr enthält.

Die Statistik umfasst Folgendes:

- Verteilung des gesperrten Datenverkehrs auf die Kategorien
- Verteilung von zugelassenem/gesperrtem Datenverkehr im zeitlichen Verlauf
- Verteilung von MP3- und großen Dateiübertragungen im zeitlichen Verlauf
- Verteilung der Bandbreitennutzung im zeitlichen Verlauf
- Aktivitätsanalyse, die für jeden Computer zeigt, wie viel Datenverkehr und geschätzte Zeit auf freigegebenen und gesperrten Datenverkehr entfällt
- Liste der gesperrten Seiten, die der betreffende Benutzer trotz Warnung besucht hat

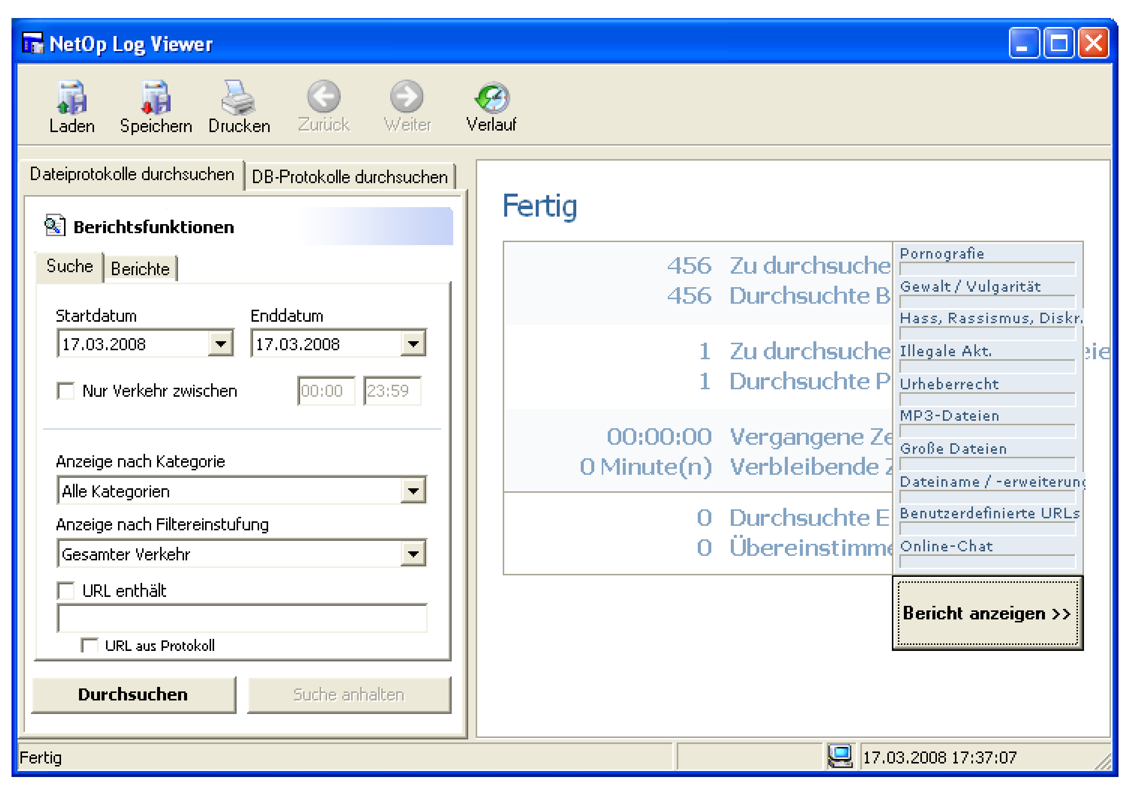


Abbildung 16: Suchen in Protokolldateien.

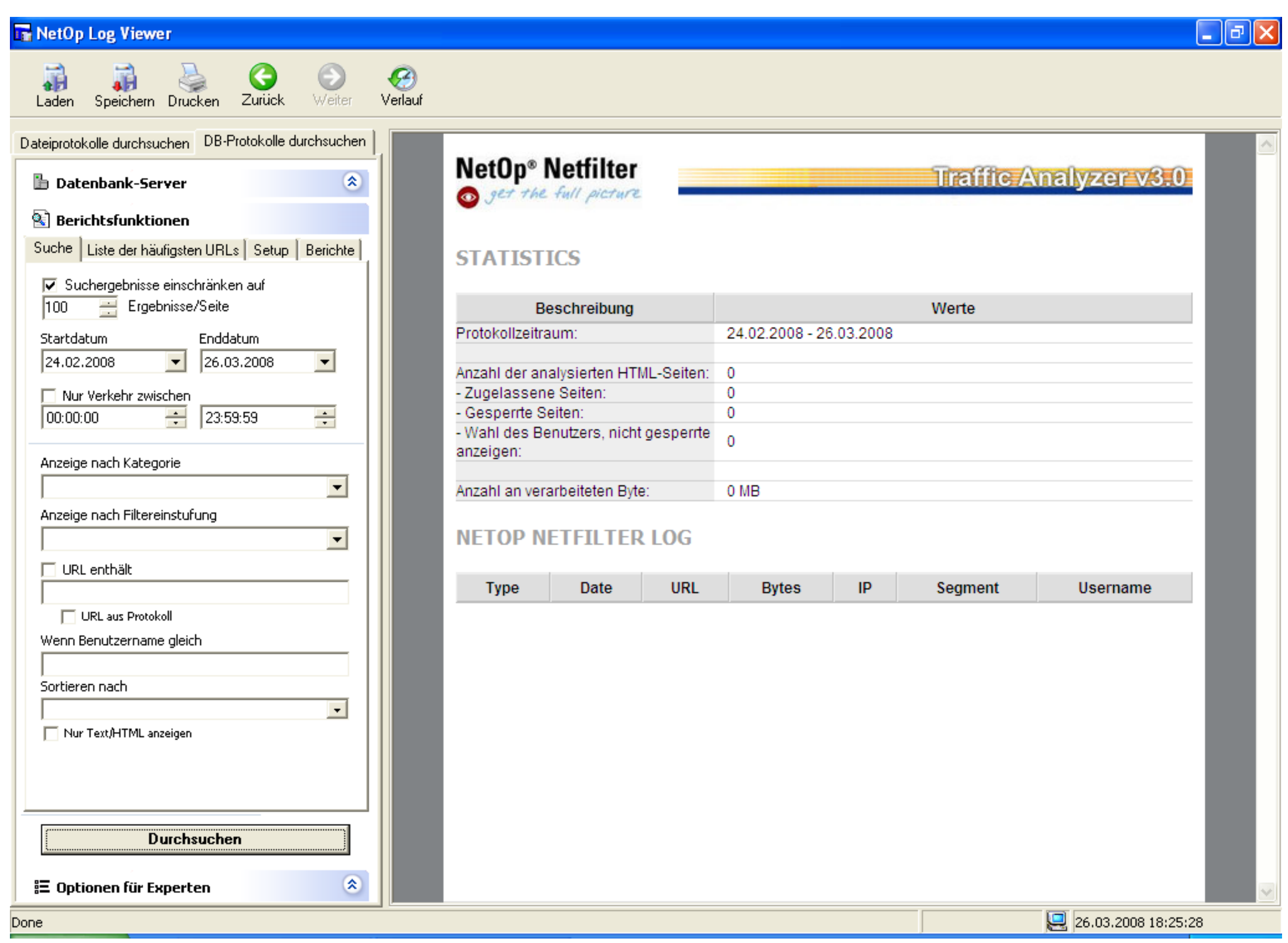


Abbildung 17: Suchen in der Datenbank.

Durch Klicken auf die Schaltfläche *Durchsuchen* wird ein Fenster geöffnet, in dem Sie nach Protokolleinträgen suchen können, die bestimmten Kriterien entsprechen (beispielsweise Datum, Uhrzeit, Kategorie und URL). NetOp Netfilter kann den Datenverkehr entweder in den lokalen Protokolldateien auf dem Server oder in einer Datenbank protokollieren. Wie in Abbildung 16 und Abbildung 17 ersichtlich, können Sie zwischen der Suche in den lokalen Protokolldateien und der Suche in der Datenbank wählen.

Wenn Sie die Protokolldateien durchsuchen, können Sie die in Abbildung 16 gezeigten Kriterien verwenden. Beachten Sie, dass Sie das Feld mit den Suchkriterien mit Hilfe des Symbols in der rechten oberen Ecke aufklappen können. Die Suche beginnt mit der Schaltfläche Protokoll durchsuchen. Die Suche in Protokolldateien kann zeitaufwändig sein. Grenzen Sie daher die Suche mit Hilfe der Suchkriterien ein. Während der Suche werden Verlaufsinformationen angezeigt. Nach Abschluss der Suche können Sie auf die Schaltfläche Protokollbericht anzeigen klicken, um den Bericht anzuzeigen.

Wenn Sie eine Datenbank durchsuchen, stehen ähnliche Suchkriterien zur Verfügung, und die Ergebnisse können auf Seiten mit beispielsweise je 100 Einträgen angezeigt werden. Auf diese Weise können Sie die Ergebnisse einsehen, bevor alle Einträge durchsucht worden sind.

Erfahrene Benutzer können unter Exportmodus-Optionen einen SQL-Editor starten, über den die Suche angepasst werden kann. Der SQL-Code wird bei einer Änderung der Suchkriterien automatisch angepasst, Starten Sie die Suche mit Hilfe der Schaltfläche Protokoll durchsuchen.

IP-Adressen werden in einem speziellen Format in der Datenbank gespeichert. Zum Übersetzen einer Adresse von der üblichen Schreibweise für IP-Adressen in dieses Format kann der IP-Rechner des SQL-Editors verwendet werden. Der Rechner wird über das Symbol IPCALC gestartet. Mit Hilfe der beiden kleinen Datenträgersymbole kann SQL-Code gespeichert und geladen werden.

Sie können die Adresse, den Namen etc. der Datenbank mit Hilfe des Felds Datenbank-Server ändern.

Über die Schaltflächen am oberen Fensterrand können Sie den aktuellen Bericht speichern bzw. ausdrucken oder einen zuvor gespeicherten Bericht laden. Mit den Schaltflächen Zurück und Weiter können Sie zwischen verschiedenen Seiten wechseln. Sie können auch zwischen Seiten wechseln, indem Sie auf die Historie am unteren Fensterrand klicken. Diese wird angezeigt, wenn die Schaltfläche Historie ausgewählt wurde.

Siehe hierzu: Fehlerbehebung

3.3.2 URL-Listen

Als URLs bezeichnet man die Adressen von Webseiten. Einige dieser Seiten enthalten unangemessene Inhalte, andere nicht. Die URLs können in Listen verwaltet werden:

Siehe hierzu: Fehlerbehebung, Liste Immer zulassen und Liste Immer sperren

3.3.2.1 Liste Immer zulassen

Über die Registerkarte Liste Immer zulassen (siehe auch Abbildung 18) können Sie URLs, die NetOp Netfilter unabhängig von ihrem Inhalt nie sperren soll, zur Liste der zulässigen URLs hinzufügen. So können Sie beispielsweise den internen Web-Server des Unternehmens hinzufügen, damit dieser nicht analysiert wird.

Wenn Sie einen URL hinzufügen möchten, geben Sie diesen in das URL-Feld ein, und klicken Sie auf *Hinzu*.

Wenn Sie einen URL entfernen möchten, wählen Sie den gewünschten URL aus, und klicken Sie auf *Entfernen*.

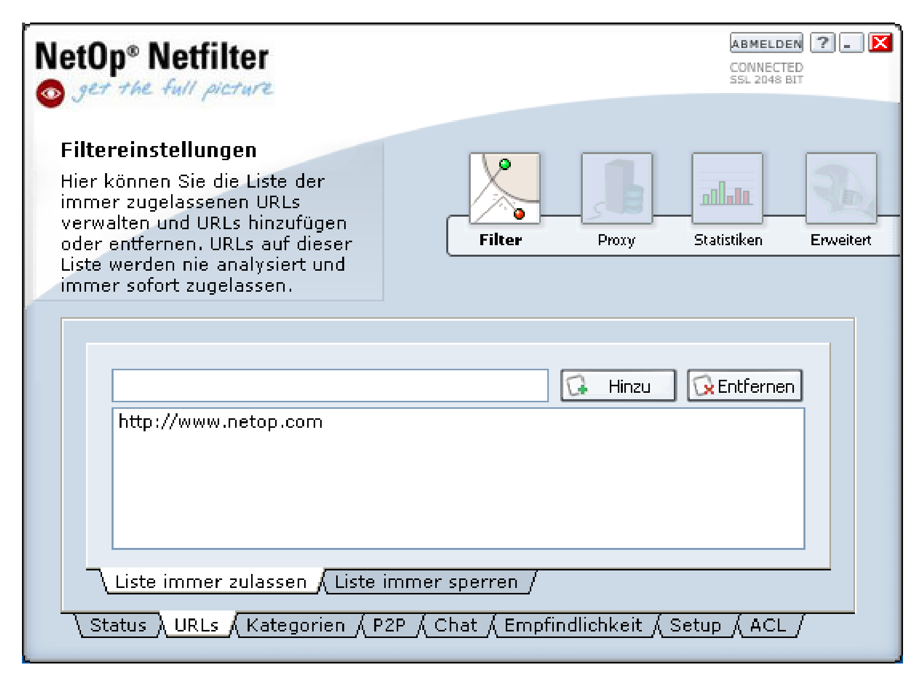


Abbildung 18: Liste "Immer zulassen". Die Internet-Adressen in dieser Liste werden nie gesperrt.

Ein URL in der Liste der zulässigen URLs gilt auch für alle untergeordneten URLs. So kann beispielsweise auf http://www.netop.com/test/ mit den Einstellungen in Abbildung 18 immer zugegriffen werden. Umgekehrt könnte http://www.test.com gesperrt sein, obwohl http://www.test.com/dirty/ zur Liste hinzugefügt wurde.

3.3.2.2 Liste Immer sperren

Über die Registerkarte Liste Immer sperren (siehe auch Abbildung 19) können Sie URLs zur Liste hinzufügen, die unabhängig von ihrem Inhalt immer gesperrt werden sollen. Auf diese Weise können Seiten hinzugefügt werden, deren Inhalte in den Standardkategorien nicht erfasst sind, wie beispielsweise Glücksspiel oder andere unerwünschte Themen.

Wenn Sie einen URL hinzufügen möchten, geben Sie diesen in das URL-Feld ein, und klicken Sie auf *Hinzu*.

Wenn Sie einen URL entfernen möchten, wählen Sie den gewünschten URL aus, und klicken Sie auf *Entfernen*.

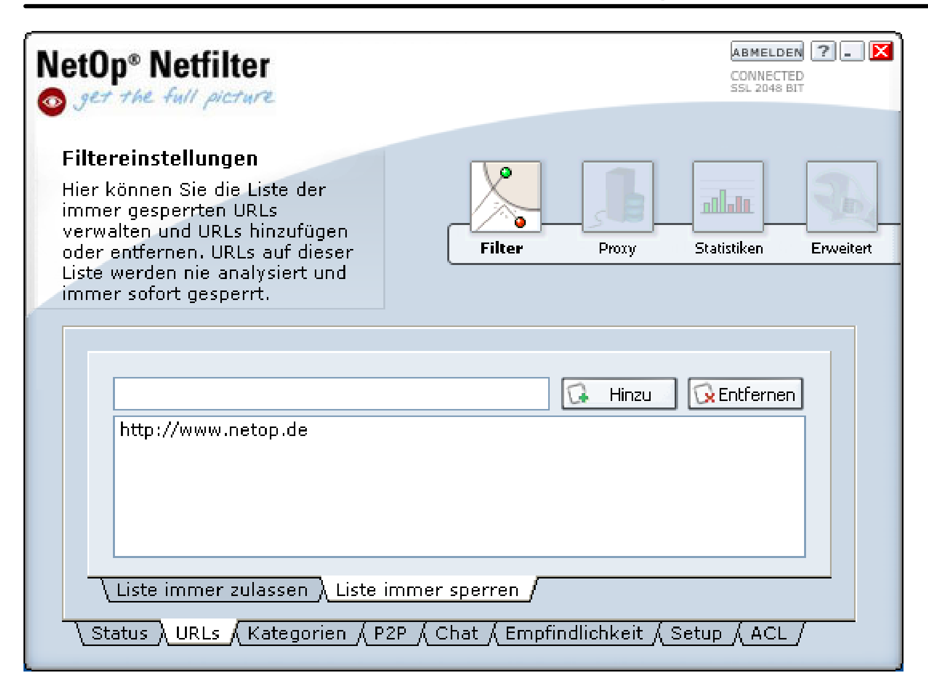


Abbildung 19: Liste "Immer sperren". Die Internet-Adressen in dieser Liste werden immer gesperrt.

Ein URL in der Liste der gesperrten URLs gilt auch für alle untergeordneten URLs. So wird beispielsweise http://www.gambling.com/test/ immer gesperrt, wenn die Einstellungen denen in Abbildung 19 entsprechen. Umgekehrt könnte http://www.test.com freigegeben werden, selbst wenn http://www.test.com/dirty/ zur Liste hinzugefügt wurde.

3.3.3 Kategorien

Auf der Registerkarte Kategorien können Sie festlegen, welche Kategorien der Filter sperren soll. Markieren Sie dazu die gewünschten Kategorien in der Liste (siehe Abbildung 20). Sobald eine Kategorie markiert ist, wird rechts im Fenster eine Beschreibung dieser Kategorie angezeigt.

Folgende Kategorien werden unterstützt:

- Pornografie. Websites mit pornografischen Inhalten. Websites zur Sexualerziehung werden nur gesperrt, wenn der Inhalt sehr detailliert oder extrem ist.
- Dating. Kontaktbörsen im Internet, dazu gehören Webseiten mit Kontaktanzeigen und Speed-Dating ebenso wie Partnerschaftsvermittlungen.
- Glücksspiel. Websites mit Glücksspielen. In erster Linie Websites, auf denen Benutzer um Geld spielen können, wie z. B. Online-Casinos und Buchmacher; die Kategorie umfasst darüber hinaus aber auch Websites, die Informationen rund um das Glücksspiel bereitstellen, wie Anleitungen, Software, Sportstatistiken und die Homepages von Casinos.
- Hass, Rassismus und Diskriminierung. Websites, auf denen aufgrund von Hautfarbe, Religion oder sexueller Orientierung Diskriminierungen gegenüber einer Gruppe geäußert werden, Hass auf diese Gruppe ausgedrückt, zu Übergriffen auf diese Gruppe aufgerufen oder auf denen eine Gruppe als einer anderen überlegen dargestellt wird.
- Gewalt und vulgärer Humor. Websites mit gewalttätigen oder anstößigen Inhalten, die sich auf Gewalt, Mord, Selbstmord, Tod, Unfälle, Krankheiten, Verstümmelungen, Kannibalismus, Nekrophilie und Körperfunktionen beziehen.
- Urheberrechtsverletzungen. Websites, die illegalen Zugriff auf Software, Filme, Musik u. ä. bieten und somit das Urheberrecht verletzen.
- Illegale oder gefährliche Aktivitäten. Websites, auf denen Anleitungen zur Herstellung/ Produktion oder illegalen bzw. gefährdenden Nutzung von Waffen, Sprengstoff,

Feuerwerkskörpern und giftigen Chemikalien sowie zu Kreditkartenbetrug, Einbruch und Diebstahl und anderen kriminellen Aktivitäten zu finden sind.

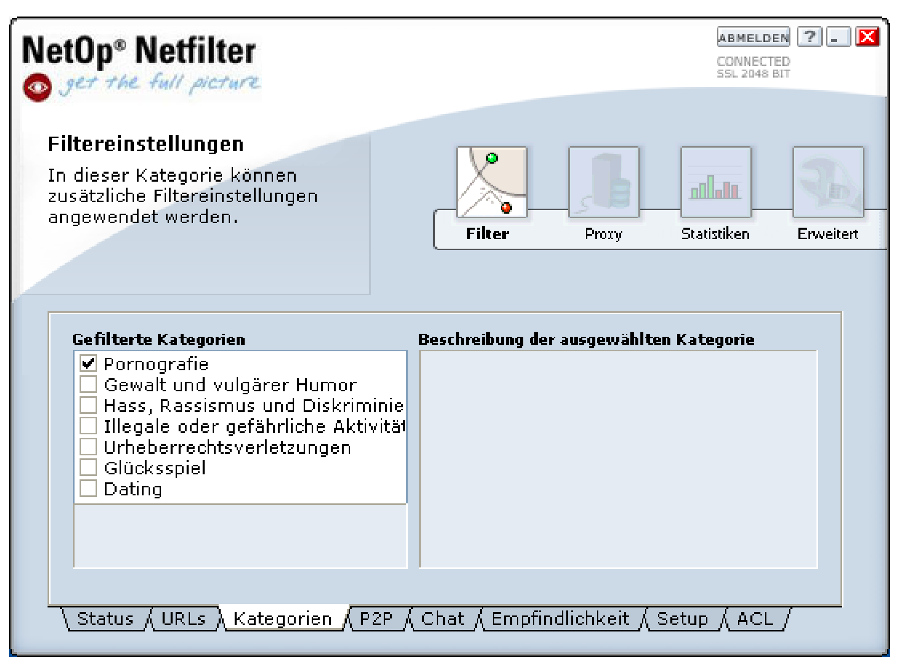


Abbildung 20: Kategorien. Der Filter sperrt die in der Liste ausgewählten Kategorien.

Siehe hierzu: Kategorien einrichten und Fehlerbehebung

3.3.4 P2P (Peer-2-Peer)

Auf der Registerkarte P2P können Sie Peer-2-Peer-Programme sperren, mit denen Software, Musik, Filme usw. im Internet ausgetauscht werden. Die beiden wichtigsten Gründe für das Sperren solcher Anwendungen sind zum Einen die Größe der ausgetauschten Dateien, deren Übertragung aufwändig ist, sowie die Tatsache, dass diese Programm häufig zur unerlaubten Verbreitung von Dateien genutzt werden.

Hinweis: Die Peer-2-Peer-Sperre kann nur dann verwendet werden, wenn ECLIENT.EXE auf den Clients ausgeführt wird.

In der Liste links im Fenster in Abbildung 21 können die Peer-2-Peer-Programme ausgewählt werden, die gesperrt werden sollen. Die Standardliste umfasst die gängigsten Peer-2-Peer-Programme; Sie können die Liste jedoch beliebig erweitern.

Wenn Sie mit der rechten Maustaste auf die Liste klicken, wird ein Menü mit den folgenden Funktionen angezeigt:

- Alle Standards sperren. Mit dieser Funktion aktivieren Sie das Sperren aller Programme in der Standardliste.
- Alle Standards zulassen. Mit dieser Funktion deaktivieren Sie das Sperren aller Programme in der Standardliste.
- Alle sperren. Über diese Funktion werden alle Programme in der Liste gesperrt, auch diejenigen, die der Benutzer hinzugefügt hat.
- Alle zulassen. Über diese Funktion wird die Sperre für alle Programme in der Liste aufgehoben, auch für diejenigen, die der Benutzer hinzugefügt hat.

Wenn Sie ein Programm zur Liste hinzufügen möchten, geben Sie den Namen der EXE-Datei oder den Fenstertitel des Programms ein. Geben Sie im Feld Beschreibung den Namen ein, unter dem das Programm in den Listen angezeigt werden soll. Fügen Sie das Programm hinzu,

indem Sie auf REGEL HINZUFÜGEN klicken.

Wenn Sie auf die Schaltfläche mit den drei Punkten rechts neben dem Textfeld des Dateinamens klicken, wird ein Fenster geöffnet, in dem Sie die Datei auswählen können.

Wenn Sie den Dateinamen und den Fenstertitel eingegeben haben, werden alle Programme mit dem entsprechenden Dateinamen oder Fenstertitel gesperrt.

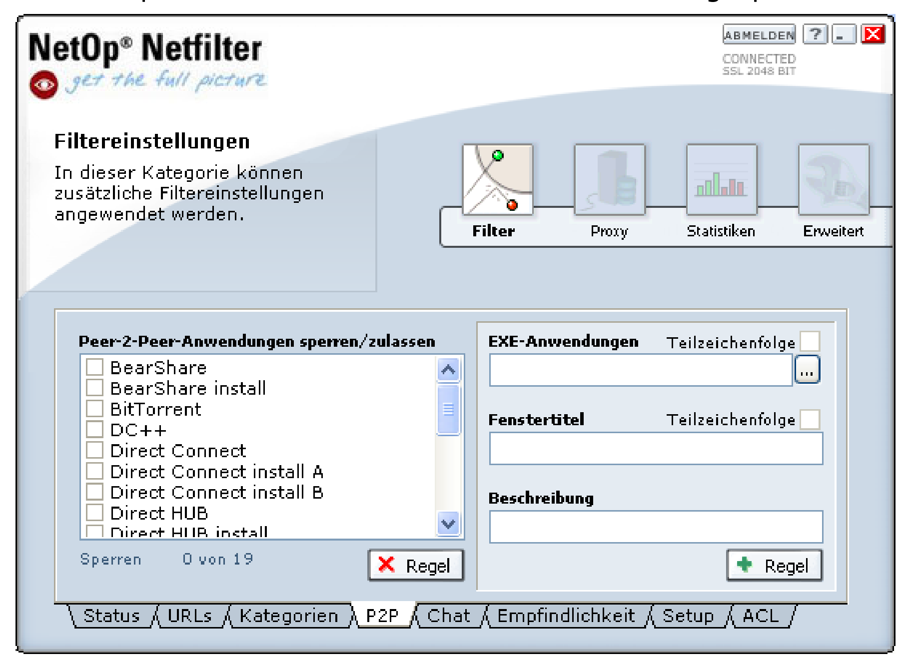


Abbildung 21: Sperren von Peer-2-Peer-Programmen.

Dateiname und Fenstertitel können auch durch Abgleichen von Teilzeichenfolgen gefiltert werden. Beim Dateinamen werden Programme gesperrt, bei denen der Name der EXE-Datei den angegebenen Text enthält. Wenn Sie beispielsweise "p2p" als Dateinamen festlegen und die Funktion Mit Teilzeichenfolge abgleichen aktivieren, werden die Dateien "p2p.exe", "myp2p.exe" und "p2p program.exe" gesperrt. In der gleichen Weise erfolgt der Zeichenabgleich beim Fenstertitel. Sie sollten diese Funktion jedoch mit Bedacht einsetzen, da Sie sonst schnell ein falsches Programm sperren.

Die Sperrfunktion führt zum Schließen der Programme. Dies kann einige Sekunden dauern. Wenn der Fenstertitel zum Abgleich verwendet wird, wird das Programm nur dann geschlossen, wenn das Fenster aktiv ist.

Programme, die vom Benutzer hinzugefügt wurden, können durch Markieren und anschließendes Klicken auf REGEL ENTFERNEN entfernt werden. Die Programme in der Standardliste können nicht entfernt werden.

Siehe hierzu: Fehlerbehebung

3.3.5 Chat-Sperre

Die Seite für die Chat-Sperre wird in Abbildung 22 gezeigt. In der Liste auf der linken Seite können die zu sperrenden Chat-Typen ausgewählt werden. Ist die Option für Browser-/Online-Chat aktiviert, werden Websites mit Chat-Angeboten gesperrt. Die übrigen Einträge in der Liste umfassen gängige Chat-Programme.

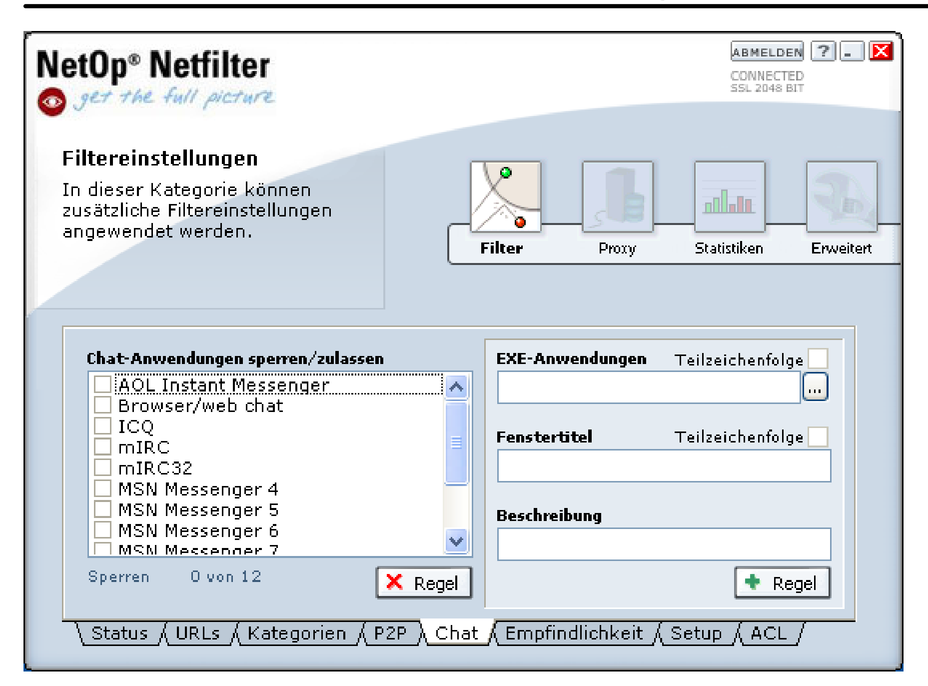


Abbildung 22: Chat-Sperre.

Hinweis: Die Chat-Sperre kann nur dann verwendet werden, wenn ECLIENT.EXE auf den Clients ausgeführt wird. Die Sperre für Browser/Online-Chat kann jedoch immer verwendet werden.

Wenn Sie mit der rechten Maustaste auf die Liste klicken, wird ein Menü mit den folgenden Funktionen angezeigt:

- Alle Standards sperren. Mit dieser Funktion aktivieren Sie das Sperren aller Programme in der Standardliste.
- Alle Standards zulassen. Mit dieser Funktion deaktivieren Sie das Sperren aller Programme in der Standardliste.
- Alle sperren. Über diese Funktion werden alle Programme in der Liste gesperrt, auch diejenigen, die der Benutzer hinzugefügt hat.
- Alle zulassen. Über diese Funktion wird die Sperre für alle Programme in der Liste aufgehoben, auch für diejenigen, die der Benutzer hinzugefügt hat.

Wenn Sie ein Programm zur Liste hinzufügen möchten, geben Sie den Namen der EXE-Datei oder den Fenstertitel des Programms ein. Geben Sie im Feld Beschreibung den Namen ein, unter dem das Programm in den Listen angezeigt werden soll. Fügen Sie das Programm hinzu, indem Sie auf REGEL HINZUFÜGEN klicken.

Wenn Sie auf die Schaltfläche mit den drei Punkten rechts neben dem Textfeld des Dateinamens klicken, wird ein Fenster geöffnet, in dem Sie die Datei auswählen können.

Wenn Sie den Dateinamen und den Fenstertitel eingegeben haben, werden alle Programme mit dem entsprechenden Dateinamen oder Fenstertitel gesperrt.

Dateiname und Fenstertitel können auch durch Abgleichen von Teilzeichenfolgen gefiltert werden. Beim Dateinamen werden Programme gesperrt, bei denen der Name der EXE-Datei den eingegebenen Text enthält. Wenn Sie beispielsweise "chat" als Dateinamen festlegen und die Funktion Mit Teilzeichenfolge abgleichen aktivieren, werden die Dateien chat.exe, mychat. exe und chat program.exe gesperrt. In der gleichen Weise erfolgt der Zeichenabgleich beim Fenstertitel. Sie sollten diese Funktion jedoch mit Bedacht einsetzen, da Sie sonst schnell ein falsches Programm sperren.

Die Sperrfunktion führt zum Schließen der Programme. Dies kann einige Sekunden dauern. Wenn der Fenstertitel zum Abgleich verwendet wird, wird das Programm nur dann

geschlossen, wenn das Fenster aktiv ist.

Programme, die vom Benutzer hinzugefügt wurden, können durch Markieren und anschließendes Klicken auf REGEL ENTFERNEN aus der Liste entfernt werden. Die Programme in der Standardliste können nicht entfernt werden.

Siehe hierzu: Fehlerbehebung

3.3.6 Empfindlichkeit

Wie in Abbildung 23 ersichtlich, können Sie über die Registerkarte Empfindlichkeit einstellen, wie sensibel NetOp Netfilter auf unerwünschte Inhalte reagieren soll. Dabei können Sie zwischen den drei Grundeinstellungen Niedrig, Normal und Hoch wählen.

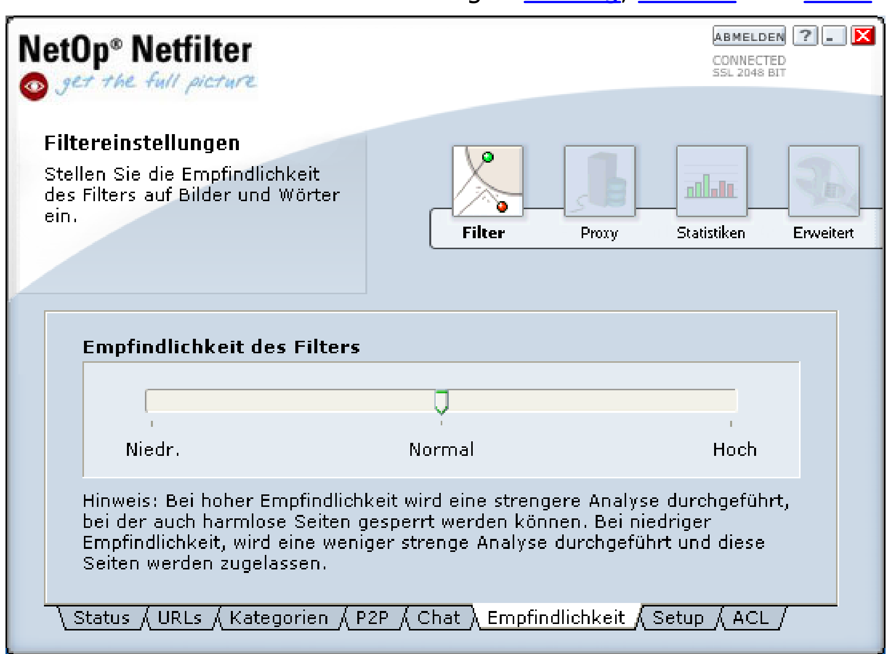


Abbildung 23: Einstellung der Filterempfindlichkeit.

Ist die Empfindlichkeitsstufe Niedrig, wird eine weniger strenge Analyse durchgeführt, d. h., es werden möglicherweise mehr Webseiten zugelassen, als durch den Filter festgelegt. Diese Einstellung eignet sich besonders, wenn Sie einen weniger restriktiven Filter verwenden möchten. Die Gefahr, dass unerwünschte Inhalte den Filter passieren, ist höher, wenn die Empfindlichkeit niedrig eingestellt ist, gleichzeitig ist aber das Risiko geringer, dass erwünschte Inhalte ungewollt gesperrt werden.

Normal ist die Standardeinstellung für den Filter und empfiehlt sich für den normalen Einsatz des Filters.

Soll eine strengere Analyse durchgeführt werden, können Sie eine höhere Empfindlichkeit auswählen. Dabei reagiert der Filter sensibler auf unerwünschte Inhalte. Allerdings werden bei dieser Einstellung sehr viele Webseiten als nicht zulässig eingestuft. Die Wahrscheinlichkeit, dass der Filter angemessene Webseiten als unangemessen einstuft, ist höher, gleichzeitig sinkt aber das Risiko, dass unerwünschte Inhalte den Filter passieren.

Siehe hierzu: Fehlerbehebung

3.3.7 Setup

Über die Registerkarte Setup können Sie verschiedene Eigenschaften des Filters aktivieren bzw. deaktivieren. Die Seite ist in eine Reihe von Registerkarten unterteilt, die sich auf die

jeweiligen Eigenschaften beziehen.

Siehe hierzu: Filter-Setup, Allgemein, Netzwerk-Setup, MP3-Analysen, Große Dateien, Dateiname/-erweit. und Protokoll-Setup

3.3.7.1 Allgemein

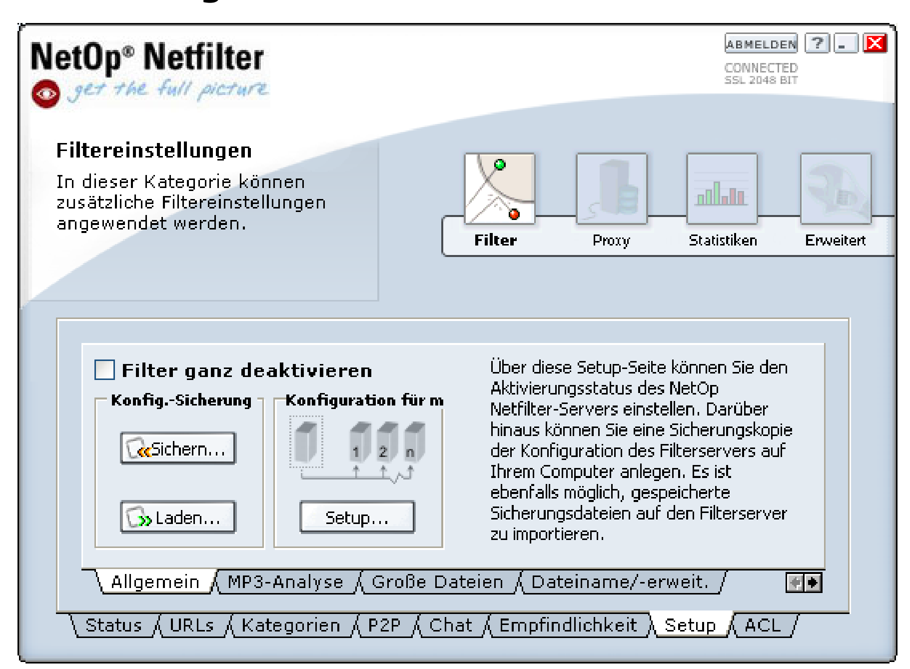


Abbildung 24: Allgemeine Filtereinstellungen.

- Filter ganz deaktivieren. Ermöglicht das Ein- und Ausschalten des Filters. Diese Option kann nützlich sein, wenn Sie vorübergehend jede Art von Datenverkehr im Netzwerk zulassen möchten.
- Konfigurations-Sicherung. Hiermit können Sie eine Konfigurationskopie lokal abspeichern, mit der Sie – bei Bedarf – die Konfiguration wiederherstellen können.
- Netzwerk-Setup. Hiermit versenden Sie das aktuelle Setup an andere Server im Netzwerk.

Siehe hierzu: Setup.

3.3.7.2 Netzwerk-Setup

Über die Option Netzwerk-Setup können mehrere Netfilter-Server gleichzeitig verwaltet werden. Dazu müssen Sie die Einstellungen auf einem Server anpassen und diese dann auf die übrigen Server übertragen. Die Server, an die die Einstellungen gesendet werden sollen, müssen in die in Abbildung 25 gezeigte Liste aufgenommen werden. Klicken Sie anschließend auf die Schaltfläche Übernehmen, um die Einstellungen auf die angegebenen Server zu übertragen.

Proxy-Einstellungen werden nur dann auf andere Server übertragen, wenn die Option *Auch Proxy-Einstellungen kopieren* ausgewählt ist.

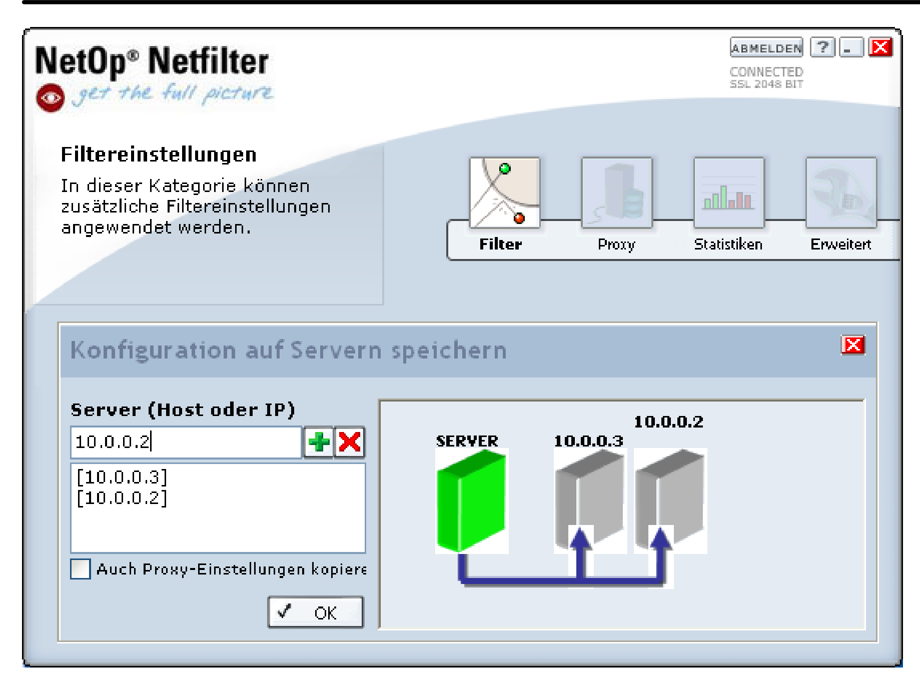


Abbildung 25: Netzwerk-Setup.

Siehe hierzu: Netzwerk-Setup.

3.3.7.3 MP3-Analyse

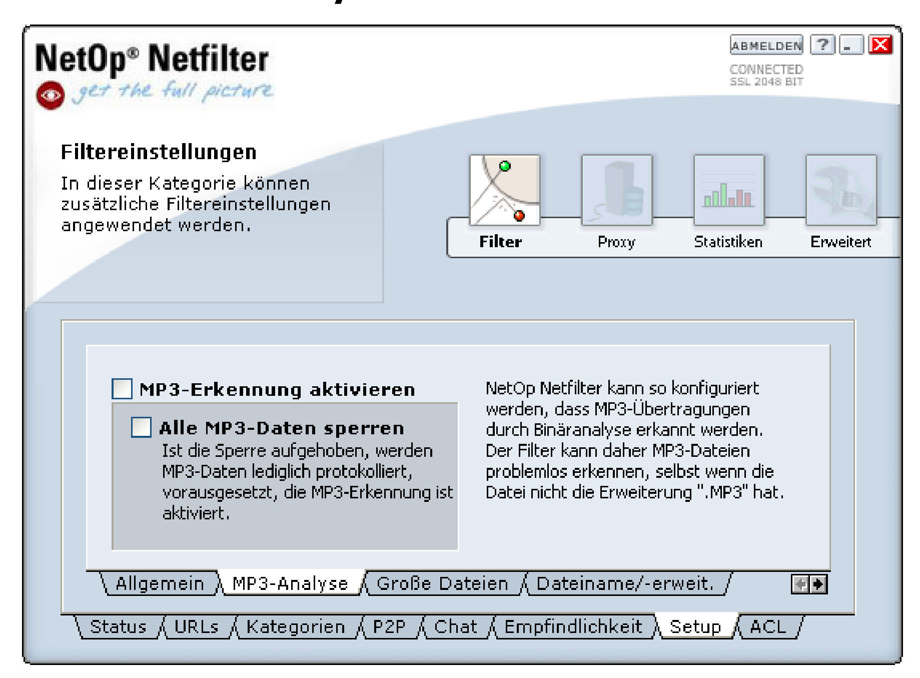


Abbildung 26: Erkennen und Sperren von MP3-Dateien.

- MP3-Erkennung aktivieren. Wenn diese Funktion aktiviert ist, wird der gesamte MP3-Verkehr in einer Protokolldatei festgehalten. Aktiviert benötigt die MP3-Erkennung mehr Ressourcen. Das Erkennen und Sperren von MP3-Dateien basiert auf Inhaltsanalysen. Das bedeutet, dass der Filter auch MP3-Dateien entdeckt, die sich als andere Formate tarnen. Die Datei MichaelJackson.gif beispielsweise wird erkannt und blockiert, wenn es sich um eine umbenannte MP3-Datei handelt.
- Alle MP3-Daten sperren. Der MP3-Verkehr wird gesperrt. Die Funktion MP3-Erkennung erfordert mehr Ressourcen.

Siehe hierzu: Filter.

3.3.7.4 Große Dateien

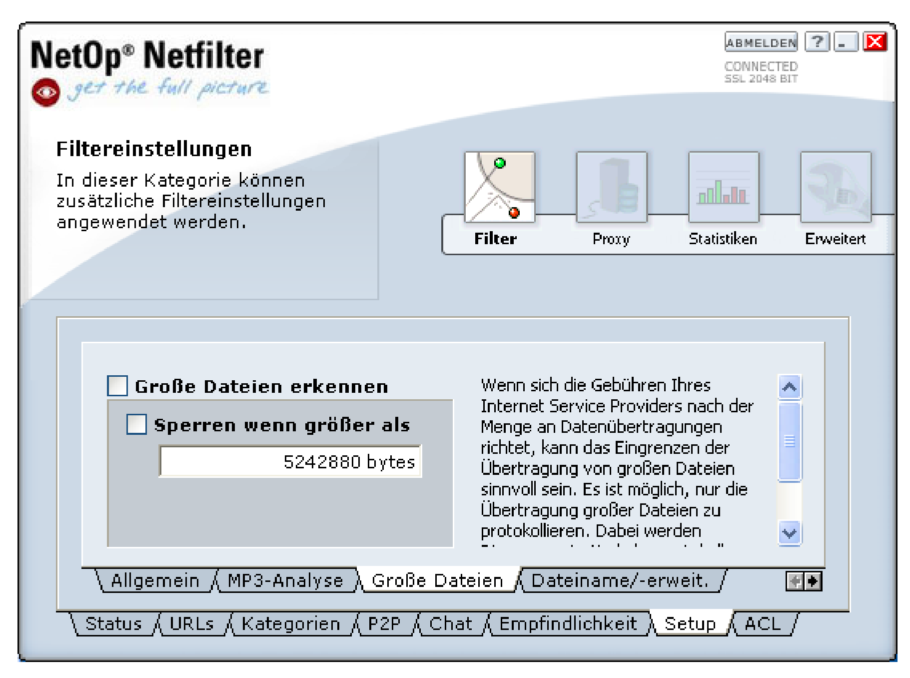


Abbildung 27: Erkennen und Sperren großer Dateien.

- Erkennung großer Dateien aktivieren. Anhand dieser Funktion können große Dateien beim Filtern erkannt werden. So kann festgestellt werden, ob solche Dateien übertragen werden. Gleichzeitig wird ein entsprechender Eintrag in der Protokolldatei erstellt. Abhängig von den Gegebenheiten können Unterschiede darin bestehen, wann eine Datei als groß einzustufen ist. Es sollte daher festgelegt werden, ab wann eine Datei als groß betrachtet wird. Die Standardeinstellungen sehen eine solche Einstufung vor, wenn eine Datei größer als 5 MB ist.
- Dateien sperren, die größer sind als. Mit dieser Funktion wird die Übertragung von Dateien gesperrt, die die festgelegte Größe überschreiten. Übertragungsversuche werden in der Protokolldatei festgehalten.

Siehe hierzu: Filter.

3.3.7.5 Dateiname/-erweit.

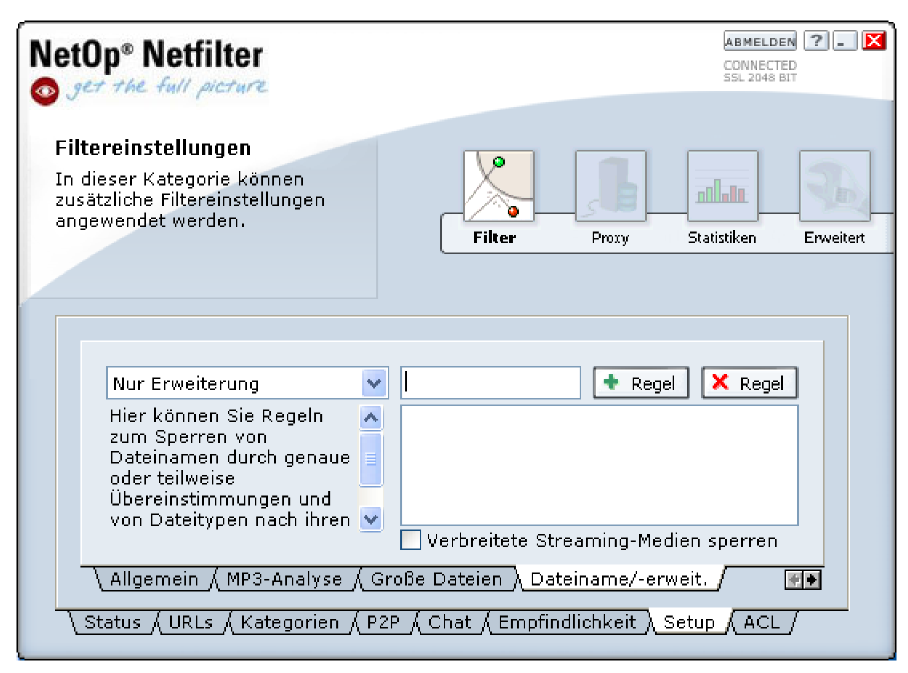


Abbildung 28: Sperren nach Namen.

Wenn die Option Verbreitete Streaming-Medien sperren aktiviert ist, werden Regeln für die gängigen Streaming-Medien hinzugefügt.

Für das Hinzufügen von Regeln stehen drei Methoden zur Auswahl:

- Nur Erweiterung. Geben Sie die Erweiterung, z. B. 'exe' oder 'zip', in das Textfeld ein, und klicken Sie auf REGEL HINZUFÜGEN, um die Erweiterung in die Liste aufzunehmen. Nun werden alle Dateien, die die festgelegte Erweiterung enthalten, gesperrt.
- Genauer Dateiname. Wenn Sie Dateien mit bestimmten Namen sperren möchten, geben Sie den Dateinamen wie z. B. 'foo.exe' in das Textfeld ein. Klicken Sie anschließend auf REGEL HINZUFÜGEN – der Dateiname wird in die Liste aufgenommen.
- Teilweise Übereinstimmung mit Dateiname. Über diese Kategorie können Sie Dateien sperren, deren Namen bestimmte Zeichenfolgen enthalten. Geben Sie die Zeichenfolge, die der Dateiname enthalten soll, in das Textfeld ein, und klicken Sie auf REGEL HINZUFÜGEN, um die Regel hinzuzufügen.

Sie können Regeln entfernen, indem Sie die entsprechende Regel auswählen und anschließend auf REGEL ENTFERNEN klicken.

Siehe hierzu: Filter.

3.3.7.6 Protokoll-Setup

Über die Seite Protokoll-Setup können Sie auswählen, welche Informationen zum Benutzer und zu den von ihm besuchten Websites protokolliert werden sollen. Standardmäßig werden nur die IP-Adressen protokolliert. Wenn im Netzwerk DNS (Domain Name Service) verwendet wird, können auch die DNS-Adressen der Clients protokolliert werden.

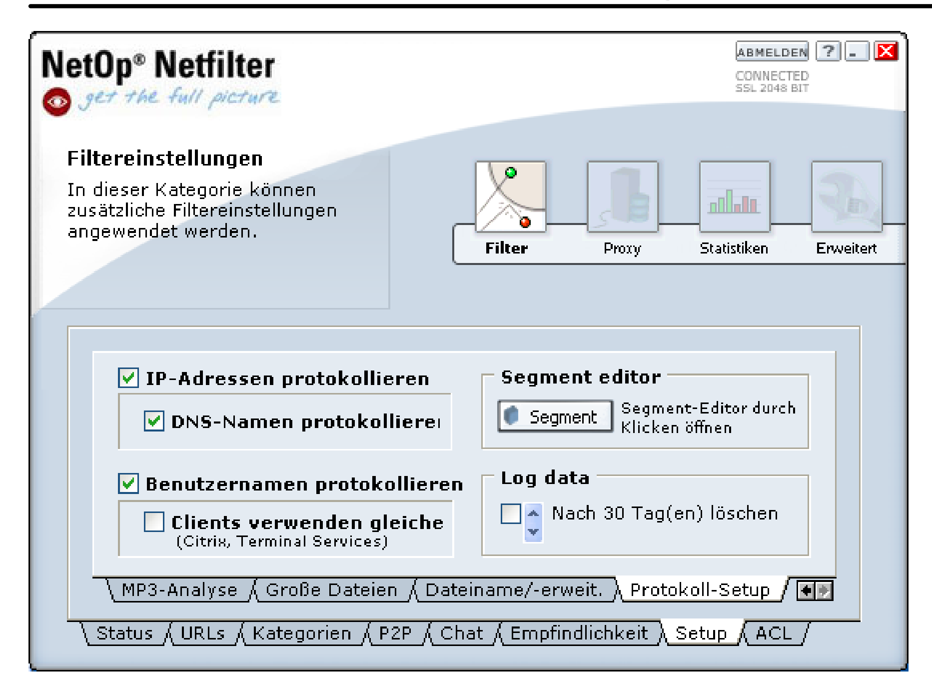


Abbildung 29: Protokollieren von Adressen und Benutzernamen.

Ist die Protokollierung von Benutzernamen aktiv, werden die Anzahl gesperrter und zugelassener Seiten und die Bandbreitennutzung je Benutzer und nicht für jede IP-Adresse protokolliert. Außerdem wird im Protokoll festgehalten, welche(r) Benutzer auf dem Computer angemeldet war(en), über den eine bestimmte Webseite aufgerufen wurde. In der Liste der Webseiten, die über den Befehl Seite zulassen und anzeigen aufgerufen wurden, wird der Name des Benutzers angezeigt, der diese Aktion durchgeführt hat. Aktivieren Sie die Protokollierung von Benutzernamen nur dann, wenn ECLIENT.EXE auf allen Clients ausgeführt wird.

Hinweis: Die Benutzernamen können nur dann protokolliert werden, wenn ECLIENT.EXE auf den Clients ausgeführt wird. Die Protokollierung von Benutzernamen wird erst aktiv, wenn ECLIENT.EXE auf allen Clients ausgeführt wird.

Sie müssen die Optionen Benutzernamen protokollieren und Clients verwenden gleiche IP-Adresse auswählen, wenn sich mehrere Clients eine IP-Adresse teilen. Außerdem muss ECLIENT.EXE mit dem Parameter /sharedip ausgeführt werden. Zur Nutzung der gleichen IP-Adresse durch mehrere Benutzer kommt es beispielsweise, wenn Citrix oder Terminal Services verwendet werden oder wenn zwischen den Benutzern und NetOp Netfilter ein weiterer Proxy-Server installiert ist.

Hinweis: Für eine ordnungsgemäße Protokollierung des Datenverkehrs bei Nutzung der gleichen IP-Adresse durch mehrere Benutzer ist es unbedingt erforderlich, dass alle Benutzer Internet Explorer als Browser verwenden.

Protokolldaten können nach einer bestimmten Anzahl von Tagen automatisch gelöscht werden, beispielsweise um den Speicherplatzverbrauch zu begrenzen. Aktivieren Sie hierzu das Kontrollkästchen Nach N Tag(en) löschen. Sie können die Anzahl von Tagen mit Hilfe der Pfeilsymbole ändern.

Wenn Sie auf die Schaltfläche SEGMENT klicken, wird ein Fenster geöffnet, in dem Sie die Aufteilung des Protokolls in Segmente definieren können. Dieser Vorgang wird im folgenden Abschnitt beschrieben.

Siehe hierzu: Segmente und Filterprotokoll-Setup.

3.3.7.6.1 Segmente

Das Protokoll kann in Segmente unterteilt werden, so dass pro Segment jeweils ein Protokoll erstellt wird. Sie können beispielsweise die einzelnen Abteilungen Ihres Unternehmens als Segmente verwenden. Jedes Segment wird nach IP-Adresse, DNS-Suffix, Benutzernamen und Gruppen definiert.

Die Unterteilung in Segmente kann nur für zukünftige Protokolle vorgenommen werden; bereits erstellte Protokolle können nicht in Segmente unterteilt werden.



Abbildung 30: Segmente.

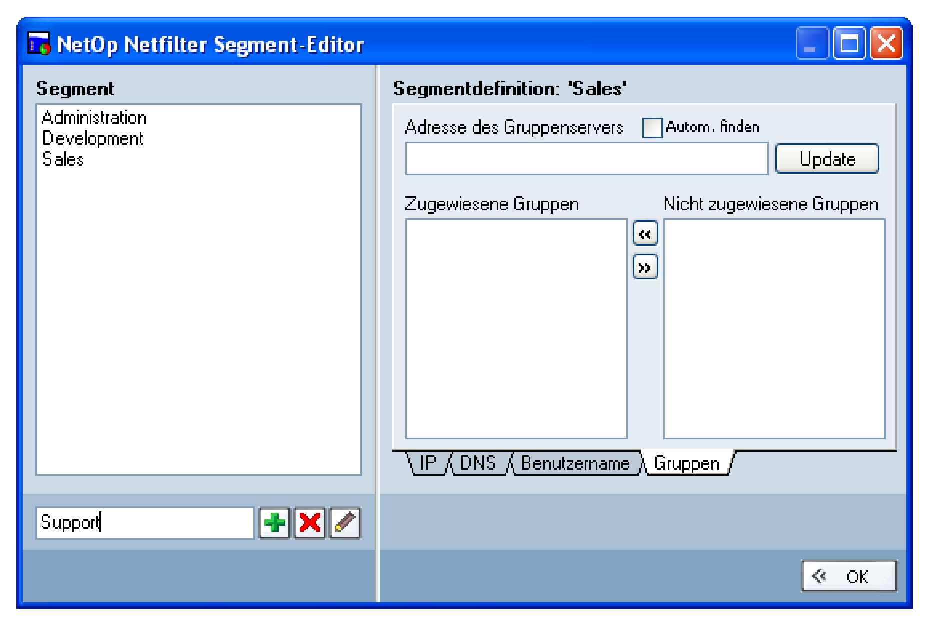


Abbildung 31: Gruppen.

Auf der linken Seite des in Abbildung 30 gezeigten Fensters sehen Sie eine Segmentliste. Wird in dieser Liste ein Segment ausgewählt, sehen Sie auf der rechten Seite, welche IP-Adressen, DNS-Adressen, Benutzernamen und Gruppen in diesem Segment protokolliert werden.

So definieren Sie ein neues Segment:

- Geben Sie unter der Segmentliste den Namen des neuen Segments ein, und klicken Sie auf

das +, um das Segment zu erstellen.

- Auf der Registerkarte IP können Sie die IP-Adressen der Computer eingeben, die in dem Segment protokolliert werden sollen. Um ein IP-Adressintervall hinzuzufügen, werden die erste und die letzte IP-Adresse des Intervalls in die beiden dafür vorgesehenen Felder eingegeben. Wenn nur eine einzelne IP-Adresse hinzugefügt werden soll, wird diese in das erste Feld eingegeben. Klicken Sie auf das +, um die Adresse bzw. das Intervall zum Segment hinzuzufügen.
- Auf der Registerkarte DNS können Sie die DNS-Suffixe der Computer eingeben, die in dem Segment protokolliert werden sollen. Geben Sie das Suffix in das Feld ein, und klicken Sie auf das +, um es zum Segment hinzuzufügen. Jetzt werden alle Computer, deren DNS-Name das angegebene Suffix enthält, im selben Segment zusammengefasst. Die angegebenen DNS-Suffixe werden nur dann verwendet, wenn die Protokollierung von DNS-Namen aktiviert wurde (siehe hierzu den Abschnitt Protokoll-Setup).
- Auf der Registerkarte Benutzername können Sie die Namen der Benutzer eingeben, die in diesem Segment protokolliert werden sollen. Geben Sie den Namen in das Feld ein, und klicken Sie auf das +, um ihn zum Segment hinzuzufügen. Die eingegebenen Benutzernamen werden nur wirksam, wenn die Protokollierung von Benutzernamen aktiviert ist.
- Auf der in Abbildung 31 gezeigten Registerkarte Gruppen können Sie die Gruppen auswählen, deren Mitglieder in dem Segment protokolliert werden sollen. Wählen Sie in der rechten Liste die gewünschte Gruppe aus, und klicken Sie auf <<, um diese hinzuzufügen. Sie können die Gruppe durch Klicken auf >> wieder aus der Gruppe entfernen.

Die Gruppenliste wird von einem Domain-Controller abgerufen. Ist die Option Autom. finden ausgewählt, versucht Netfilter, einen Domain-Controller zu finden. Andernfalls müssen Sie die Adresse des Domain-Controllers unter Adresse des Gruppenservers angeben. Wird ein Domain-Controller angegeben und die Option Autom. finden ausgewählt, wird der angegebene Domain-Controller (sofern verfügbar) verwendet. Andernfalls versucht Netfilter, einen anderen Domain-Controller zu ermitteln. Aus diesem Grund wird empfohlen, die Option Autom. finden auch dann zu aktivieren, wenn eine Adresse eingegeben wurde.

Überschneidungen der einzelnen Segmente sind zulässig. So kann beispielsweise ein Benutzername in mehreren Segmenten eingetragen sein.

Wenn Sie ein Protokoll für einen bestimmten Benutzer erstellen möchten, können Sie ein Segment erstellen, das ausschließlich den Namen dieses Benutzers enthält.

Wenn Sie ein IP-Intervall, ein DNS-Suffix oder einen Benutzernamen in der Segmentdefinition ändern oder löschen möchten, müssen Sie dieses Element in der Liste auswählen. Anschließend können Sie dieses Element löschen, indem Sie auf ENTFERNEN klicken, oder es ändern, indem Sie den neuen Wert eingeben und auf klicken.

Wenn Sie ein Segment umbenennen möchten, wählen Sie es aus der Liste aus, und geben Sie den neuen Namen ein. Klicken Sie anschließend auf .

Um ein Segment zu löschen, wählen Sie es aus der Liste aus, und klicken Sie auf ENTFERNEN.

Auf der Registerkarte Segment überprüfen können Sie die Segmente anzeigen, in denen eine IP-Adresse, eine DNS-Adresse oder ein Benutzername protokolliert wird. Geben Sie dazu die Adresse bzw. den Namen ein, wählen Sie den Datentyp, und klicken Sie auf TEST. Die Segmente, in denen die Adresse oder der Name protokolliert werden, sind nun in der Segmentliste markiert.

3.3.8 ACL

Über die Registerkarte ACL können Sie festlegen, welche Computer in welchem Umfang auf das Internet zugreifen können. Dies wird mit Hilfe einer Access Control List (Zugangskontrollliste) definiert (siehe Abbildung 32). Sie können die IP-Adresse eines

Computers oder einen Bereich von IP-Adressen für mehrere Computer angeben und auswählen, welche Art der Filterung Sie für diese(n) Computer wünschen. Sie können zwischen drei Arten der Filterung wählen:

Immer filtern	Der Datenverkehr der angegebenen IP-Adressen wird stets gefiltert.
Ungefiltert	Der Datenverkehr der angegebenen IP-Adressen wird nie gefiltert.
Zugriff verweigert	Den angegebenen IP-Adressen wird der Zugriff auf das Internet verweigert.

Mit diesen drei Filterarten können Sie das Netzwerk sehr genau kontrollieren. In einem Unternehmen kann beispielsweise die Buchhaltung einen IP-Adressbereich belegen und die Entwicklungsabteilung einen anderen. Mit der Option ACL und nur zwei Regeln kann der gesamte Datenverkehr der Computer in der Buchhaltung gefiltert werden, während alle Computer in der Entwicklungsabteilung ungehindert auf das Internet zugreifen können. Sollen Teile des Unternehmens nicht auf das Internet zugreifen können, verwenden Sie hierzu die Regel *Zugriff verweigert*.

Wenn Sie eine einzelne IP-Adresse hinzufügen möchten, geben Sie diese ein, und klicken Sie auf die Schaltfläche REGEL HINZUFÜGEN. Wenn Sie einen IP-Adressbereich hinzufügen möchten, markieren Sie das Kontrollkästchen IP-Bereich. Sie können nun zwei IP-Adressen eingeben. Soll beispielsweise der Datenverkehr der Computer 10.0.0.1 bis 10.0.0.50 gefiltert werden, geben Sie im oberen Feld die Adresse 10.0.0.1 und im unteren Feld die Adresse 10.0.0.50 ein.

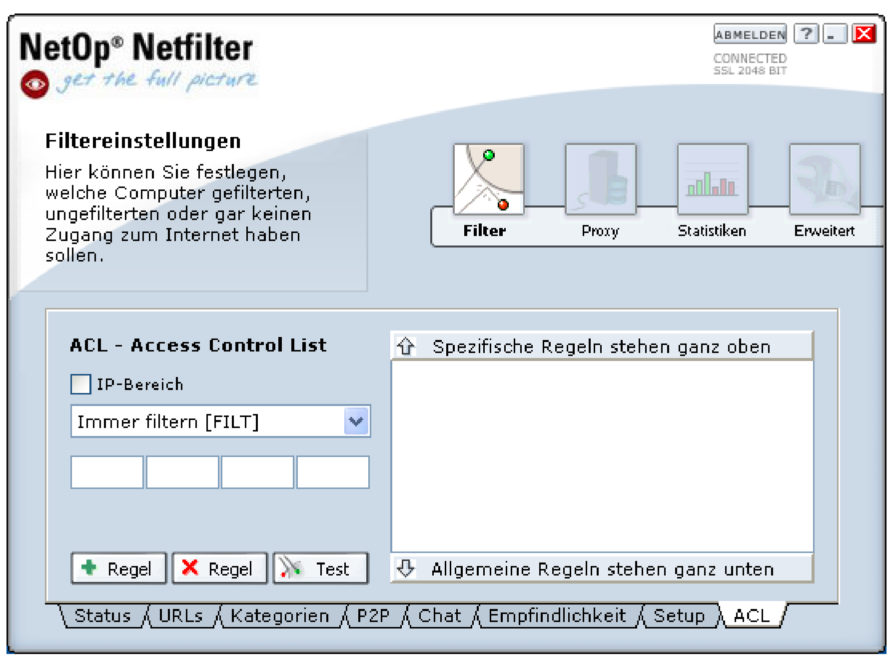


Abbildung 32: Konfigurieren der Access Control List.

Wenn Sie eine Regel entfernen möchten, wählen Sie diese mit der Maus aus, und klicken Sie auf die Schaltfläche REGEL ENTFERNEN.

Wenn Sie prüfen möchten, ob die Regeln korrekt definiert wurden, können Sie mit Hilfe der Schaltfläche TEST ermitteln, ob eine bestimmte IP-Adresse von einer oder mehreren Regeln erfasst wird. Dies ist vor allem dann nützlich, wenn komplexe Regeln erstellt wurden und fraglich ist, ob eine IP-Adresse wie gewünscht gefiltert wird.

Hinweis: Achten Sie darauf, die Ausnahmeregeln zuerst einzugeben. Wenn Sie beispielsweise alle IP-Adressen in einem Bereich mit einer Ausnahme filtern möchten, definieren Sie eine Regel, die diese Adresse von der Filterung ausschließt. Definieren Sie anschließend unterhalb dieser Regel eine zweite Regel, nach der der gesamte IP-Adressbereich gefiltert wird.

Siehe hierzu: Access Control List (Zugangskontrollliste) und Fehlerbehebung

3.4 Erweitert

In Abbildung 35 ist ein Screenshot zu Erweitert zu sehen. Hier können Sie die erweiterten Eigenschaften von *NetOp Netfilter Admin* und *NetOp Netfilter* festlegen. Über die drei Registerkarten unter *Erweitert* können Sie jene Eigenschaften anpassen, die unter normalen Umständen unverändert bleiben sollten.

Siehe hierzu: Netfilter Admin-Einstellungen, Client-Befehle, Sperrseite, Cache, Zeitplan und Konten und Berechtigungen

3.4.1 Netfilter Admin-Einstellungen

Über die in Abbildung 35 gezeigte Registerkarte können Sie die Eigenschaften von NetOp Netfilter Admin konfigurieren. Sie können mit Hilfe des Kontrollkästchens *Erweiterte Einstellungen anzeigen* festlegen, ob die erweiterten Konfigurationsoptionen angezeigt werden sollen. Die erweiterten Optionen werden standardmäßig angezeigt. Ist dieses Kontrollkästchen nicht aktiviert, ist die Benutzerschnittstelle übersichtlicher, verfügt aber auch über weniger Funktionen.

Sie können die von NetOp Netfilter verwendete Datenbank ändern. Klicken Sie dazu auf die Schaltfläche *Setup*, geben Sie im nun angezeigten Fenster die Adresse, den Benutzernamen, das Kennwort und den Namen der Datenbank ein. Wenn Sie die Datenbank nicht verwenden möchten, lassen Sie diese Parameter offen. Die Daten werden dann in lokalen Protokolldateien auf dem Netfilter-Server registriert.

Über die Option Konten und Berechtigungen können Sie mehrere Benutzerkonten einrichten und diesen verschiedene Berechtigungen zuweisen.

Mit Hilfe eines Zeitplans können für die unterschiedlichen Wochentage und Tageszeiten verschiedene Filtereinstellungen verwendet werden. Aktivieren Sie die Funktion Zeitplan mit täglichem Zeitlimit verwenden und klicken Sie anschließend auf Zeitplan, um Zeitpläne zu erstellen.

Sie können die Klickgeräusche für Schaltflächen deaktivieren.

Mit Hilfe der Option Automatische Abmeldung bei Platzierung in Taskleiste können Sie festlegen, ob sich das Programm vom Filter-Server abmelden soll, wenn NetOp Netfilter Admin minimiert wird. Damit wird gewährleistet, dass Sie abgemeldet sind, wenn Sie den Computer verlassen.

Über SSL-Verbindung prüfen können Sie festlegen, ob NetOp Netfilter Admin regelmäßig überprüfen soll, ob die verschlüsselte Verbindung zwischen NetOp Netfilter Admin und NetOp Netfilter offen ist. Sie können außerdem bestimmen, in welchen Abständen NetOp Netfilter Admin diese Prüfung durchführen soll.

Ändern Sie Benutzernamen und Kennwort, indem Sie sie in den entsprechenden Feldern rechts im Fenster eingeben. Beachten Sie, dass Sie das neue Kennwort unter *Neues Kennwort bestätigen* erneut eingeben müssen, um Fehler bei der Kennworteingabe zu vermeiden. Wenn Sie auf OK geklickt haben, werden Sie aufgefordert, Ihr aktuelles Kennwort erneut einzugeben. Geben Sie dieses Kennwort ein, und klicken Sie auf OK, um die Kennwortänderung abzuschließen.

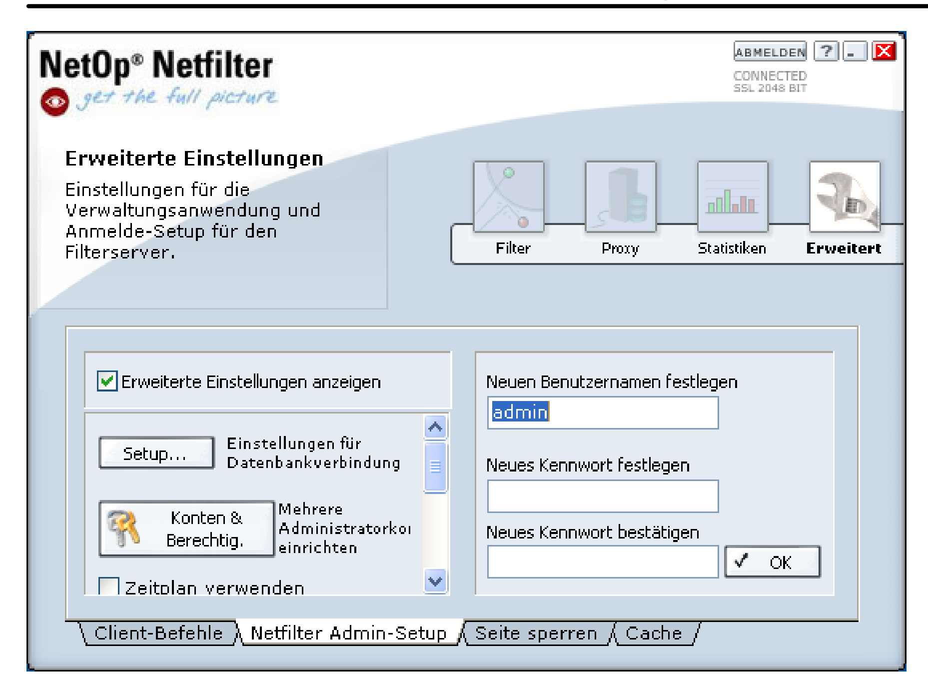


Abbildung 35: Erweiterte Einstellungen für NetOp Netfilter Admin.

Siehe hierzu: Fehlerbehebung

3.4.2 Client-Befehle

Mit Hilfe der Registerkarte Client-Befehle (siehe Abbildung 36) können Sie die Eigenschaften der Sperrseite ändern, die angezeigt wird, wenn auf unerwünschte Inhalte zugegriffen wird. Wenn das Feld Interaktive Client-Befehle auf der 'gesperrten Seite' *aktivieren* markiert ist, werden alle aktiven Befehle auf der Sperrseite angezeigt.

Der Befehl Seite zulassen und anzeigen erweitert die Sperrseite um eine zusätzliche Schaltfläche. Mit dieser Schaltfläche können Sie nun von der Sperrseite aus auf die Inhalte zugreifen, die als unangemessen eingestuft wurden. Die Sperrseite enthält den Hinweis, dass dieser Vorgang im Protokoll registriert wird. Der Befehl wird aktiviert, indem Sie ihn mit der Maus markieren und auf die Schaltfläche AKTIVIEREN klicken. Zur Deaktivierung klicken Sie auf DEAKTIVIEREN.

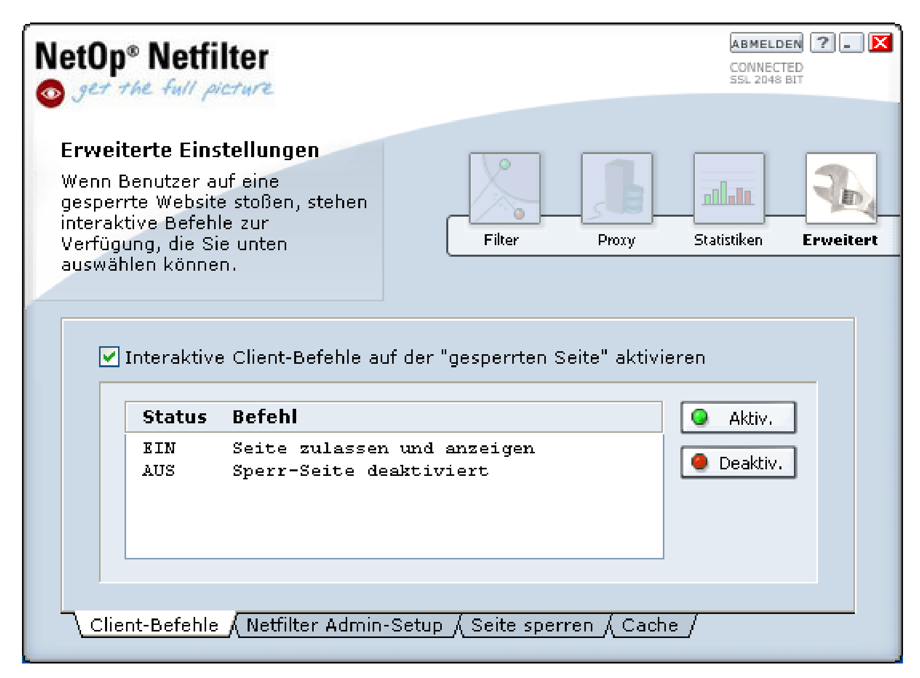


Abbildung 36: Konfigurieren von Client-Befehlen.

Dieser Befehl lässt dem Benutzer die Wahl, die betreffende Seite abzurufen oder nicht. Dieser Befehl ist beispielsweise dann nützlich, wenn der Benutzer aus beruflichen Gründen auf eine Seite zugreifen muss, die der Filter als unangemessen einstuft. In diesem Fall muss der Benutzer nicht den Administrator bitten, die Seite zu prüfen, sondern kann einfach mit seiner Arbeit fortfahren.

Wenn der Befehl Sperr-Seite deaktiviert ausgewählt wird, erfolgt keine Sperrung der besuchten Seiten. Allerdings wird der Zugriff im Protokoll festgehalten.

Siehe hierzu: Fehlerbehebung

3.4.3 Sperrseite

Wie in Abbildung 37 gezeigt, können Sie die Sprache der Sperrseite ändern. Sie haben die Wahl zwischen den aufgeführten Sprachen. Die Sperrseite wird anstelle der angeforderten Seite angezeigt, wenn NetOp Netfilter diese als unangemessen einstuft.

Außerdem können Sie die Standard-Sperrseite durch eine Seite ersetzen, die auf einer HTML-Vorlage basiert.

Wenn Sie eine Vorlage verwenden möchten, müssen Sie die Optionen Vorlage importieren und HTML-Vorlage verwenden auswählen.

Hinweis: [%%]-Befehle ersetzen die gesamte Zeile, {%%}-Befehle ersetzen nur das Tag.

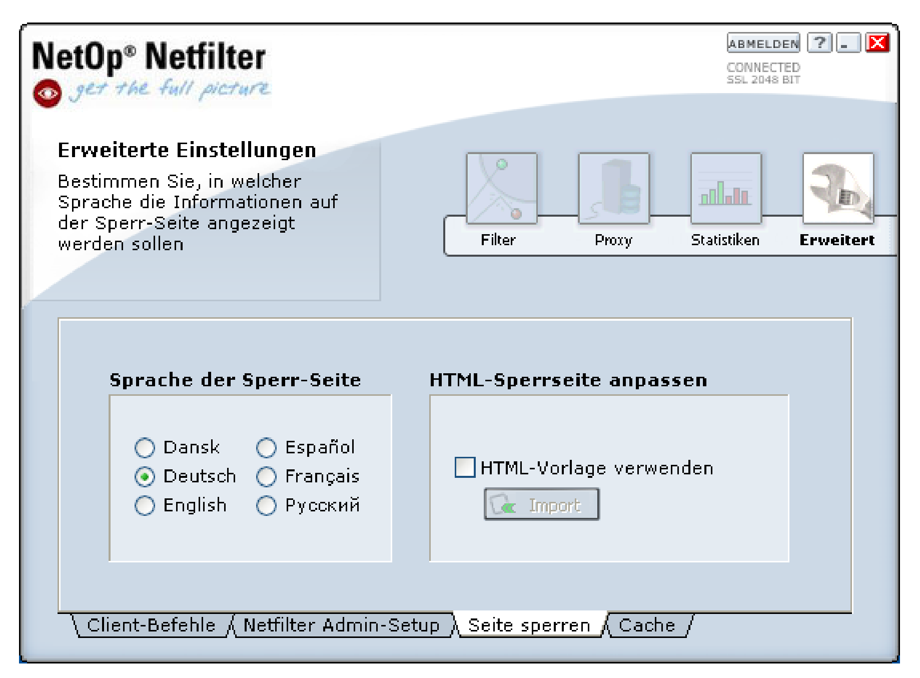


Abbildung 37: Konfigurieren der Sperrseite.

Siehe hierzu: Fehlerbehebung

3.4.4 Cache

NetOp Netfilter speichert die besuchten Websites in einem Cache-Speicher, um bei einem erneuten Besuch schneller darauf zugreifen zu können.

So löschen Sie den Inhalt dieses Cache: Wählen Sie *Erweitert* > *Cache* , und klicken Sie dann auf *Reset.*

Die über der Schaltfläche Reset angezeigten Zahlen beziehen sich auf den Festplatten- und Laufwerksspeicher, der für den Cache verwendet wird.

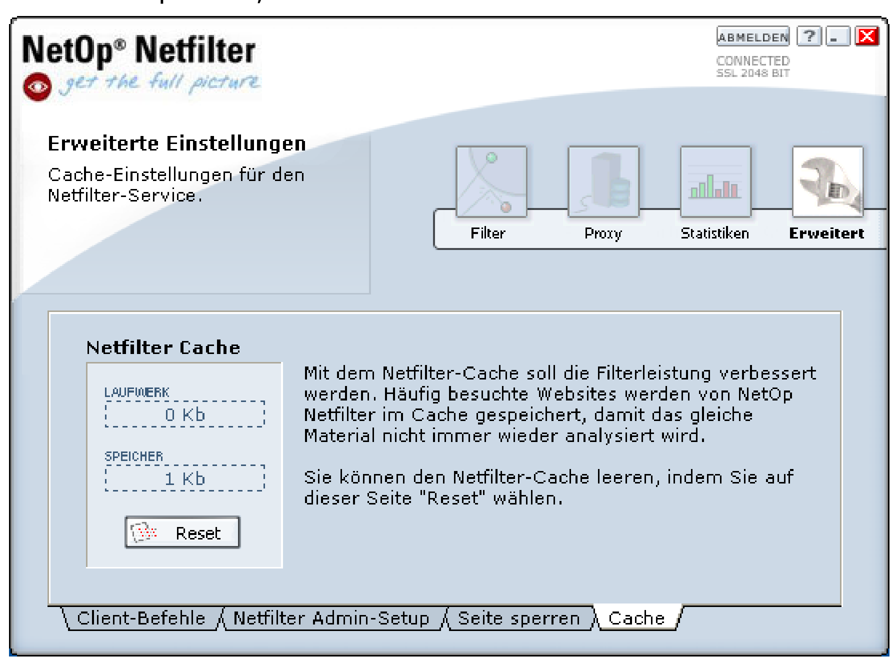


Abbildung 38: Cache.

Siehe hierzu: Fehlerbehebung

3.4.5 Zeitplan

Mit NetOp Netfilter können Sie bestimmte Einstellungen auf Grundlage eines Zeitplans programmieren. Zu diesen Einstellungen zählen der Internet-Zugriff bestimmter Segmente, die Aktivierung des Filters und die Inhalte, die der Filter sperren soll.

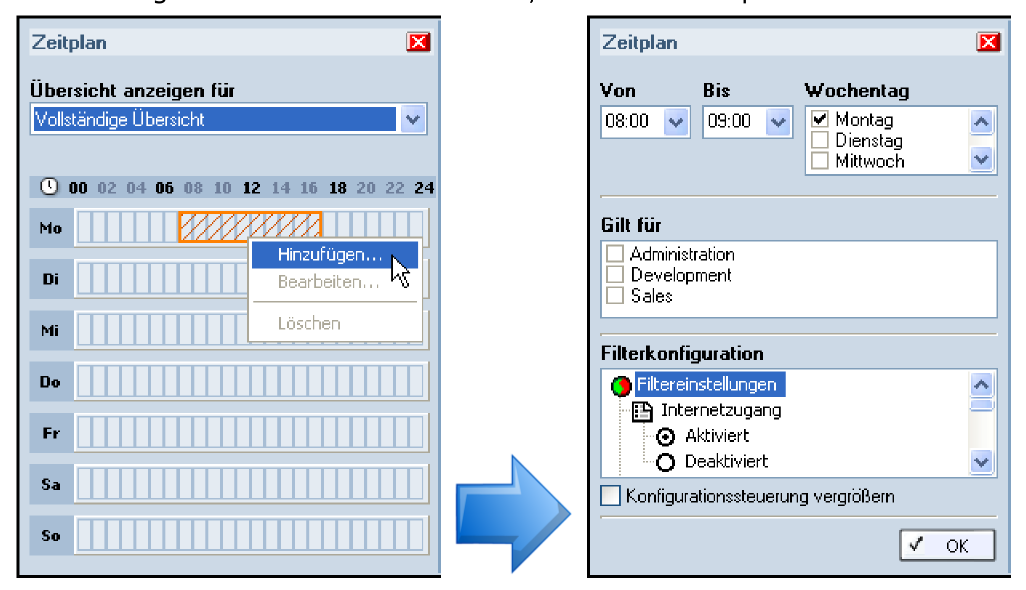


Abbildung 39: Zeitplan.

Wenn Sie einen Zeitplan aktivieren möchten, aktivieren Sie die Option *Zeitplan verwenden* auf der Seite Netfilter Admin-Setup unter *Erweitert*. Klicken Sie auf die Schaltfläche *ZEITPLAN*, um den Zeitplan zu ändern.

Wenn kein Zeitplan erstellt wurde, werden die im Hauptfenster (siehe vorherige Abschnitte) festgelegten Einstellungen verwendet. Wurden im Zeitplan Blöcke definiert, haben diese Vorrang vor den Einstellungen im Hauptfenster.

Sie können einen Block festlegen und Einstellungen dafür im Zeitplan vornehmen. Klicken Sie dazu auf ein Zeitfeld, um den Beginn des Zeitraums zu markieren, und ziehen Sie die gedrückte Maustaste über den gewünschten Zeitraum. Klicken Sie nach dem Markieren des Zeitraums mit der rechten Maustaste auf den markierten Bereich, und wählen Sie die Option *Hinzufügen...*. Der Inhalt des Fensters wechselt dann zur Einstellungssteuerung (im rechten Bereich von Abbildung 39).

Über die Einstellungssteuerung können Sie Anfang und Ende des Zeitraums anpassen und auswählen, an welchen Wochentagen die gewählten Einstellungen gelten sollen. Sie können außerdem auswählen, auf welche Segmente diese Einstellungen angewendet werden sollen. Dies bedeutet, dass für verschiedene Segmente zur gleichen Zeit unterschiedliche Einstellungen gelten können.

Die Einstellungen für den gewählten Zeitraum können in der Liste am unteren Fensterrand bearbeitet werden. Weitere Informationen zu diesen Einstellungen finden Sie im vorherigen Abschnitt.

Wenn Sie die zu verwendenden Einstellungen und Segmente sowie den Zeitraum angegeben haben, klicken Sie auf *ÜBERNEHMEN*. Auf diese Weise gelangen Sie zurück zum Zeitplan, wo Sie neue Blöcke hinzufügen, die Einstellungen vorhandener Blöcke ändern und Blöcke löschen können.

Um die Einstellungen für einen Block zu ändern, rufen Sie das Kontextmenü des entsprechenden Blocks mit der rechten Maustaste auf, und klicken Sie auf *Bearbeiten...*. Wenn

Sie einen Block aus dem Zeitplan entfernen möchten, klicken Sie im Kontextmenü auf Löschen.

Wenn Sie den Zeitplan für ein bestimmtes Segment anzeigen möchten, wählen Sie im oberen Fensterbereich das betreffende Segment im Listenfeld aus.

Um das Zeitplanfenster zu schließen, klicken Sie auf die Schaltfläche X am rechten oberen Fensterrand.

Siehe hierzu: Fehlerbehebung

3.4.6 Konten und Berechtigungen

Sie können verschiedene Benutzerkonten erstellen und verschiedenen Benutzergruppen von Netfilter Admin unterschiedliche Rechte zuweisen.

Benutzerkonten werden über das in Abbildung 40 gezeigte Fenster verwaltet. Im oberen Fensterbereich wird eine Liste der Benutzergruppen angezeigt. Im unteren Bereich wird angezeigt, zu welcher Gruppe welcher Benutzer gehört.

Wenn Sie eine neue Gruppe hinzufügen möchten, klicken Sie auf *Hinzufügen…*. Daraufhin erscheint ein neues Fenster, in dem der Name, die Beschreibung und die Berechtigungen der Gruppe ausgewählt werden. Siehe hierzu auch Abbildung 41. Das gleiche Fenster kann später durch Auswahl der Gruppe und der Option *Eigenschaften* geöffnet werden. Gruppen, denen keine Benutzer zugewiesen wurden, können durch Auswählen von *Entfernen* gelöscht werden.

Sie können einer Gruppe die Berechtigung zur Änderung der Listen Immer sperren und Immer zulassen oder einen uneingeschränkten Zugriff auf alle Einstellungen zuweisen.

Über die Schaltfläche *Hinzufügen…* unter der Liste der Benutzerkonten kann ein neuer Benutzer hinzugefügt werden. Im daraufhin angezeigten Fenster werden Name, Kennwort, Gruppe und andere Einstellungen ausgewählt. Siehe hierzu auch Abbildung 42 und Abbildung 43. Soll das Benutzerkonto nach einer bestimmten Zeit automatisch ablaufen, wählen Sie die Option *Das Konto ist gültig bis zum* aus, und geben Sie das Ablaufdatum und die Uhrzeit ein. Bei Gruppen können die Benutzereigenschaften über *Eigenschaften* angezeigt werden, und ein Benutzer lässt sich mit der Option *Entfernen* löschen.



Abbildung 40: Konten & Berechtigungen.



Abbildung 41: Eigenschaften der Gruppe.

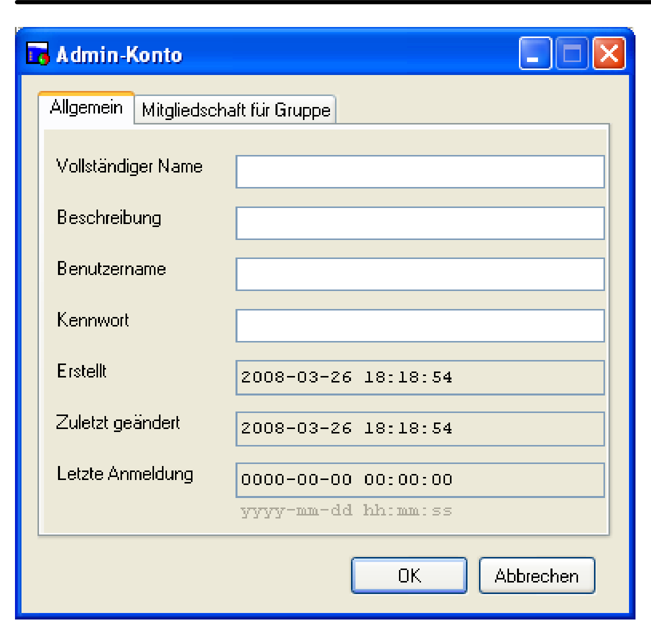


Abbildung 42: Eigenschaften des Benutzers.



Abbildung 43: Eigenschaften des Benutzers.

Siehe hierzu: Fehlerbehebung

3.5 Statistik

Wie in der linken Spalte in Abbildung 34 ersichtlich, haben Sie Zugriff auf verschiedene Filterinformationen. Diese Informationen werden nachfolgend erläutert. Alle Daten in dieser Spalte beziehen sich auf den Zeitraum vom letzten Neustart bis jetzt.

Ca. Treffer/ Sek	Die durchschnittliche Anzahl von Treffern pro Sekunde. Ein Treffer ist gleichbedeutend mit dem Aufruf einer Internet-Seite.
Max. Treffer/ Sek	Die maximale Anzahl von Treffern pro Sekunde.
Gesamttreffer	Die Gesamtzahl aller Treffer.

Zugelassene Treffer	Die Anzahl aller Anforderungen, die der Filter zugelassen hat.
Gesperrte Treffer	Die Anzahl aller Anforderungen, die der Filter gesperrt hat.
Offene Sitzungen	Die Anzahl der Sitzungen (Client-Verbindungen), die derzeit in NetOp Netfilter aktiv sind.
Durchschn. Bytes/Sek	Die durchschnittliche Datenmenge, die pro Sekunde über NetOp Netfilter geleitet wird.
Max. Kb/Sek.	Die maximale Datenmenge, die in einer Sekunde über NetOp Netfilter geleitet wurde.
Gesamt Kb	Die gesamte Datenmenge, die seit dem letzten Neustart durch den Filter geleitet wurde.

Die Einheit Byte wird mit wachsender Datenmenge in KB und dann in MB geändert.

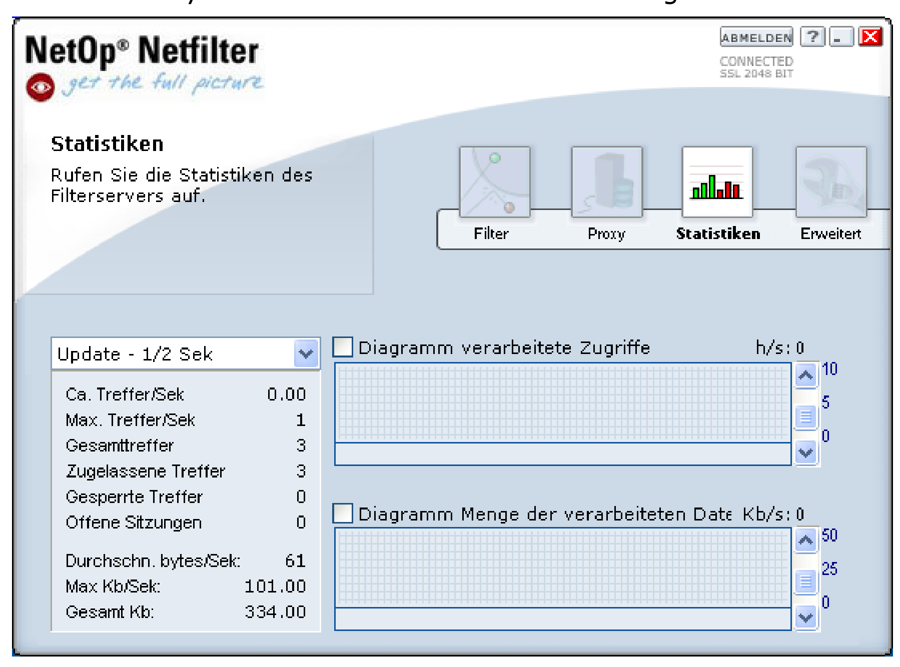


Abbildung 34: Statistik für NetOp Netfilter.

Siehe hierzu: Diagramme und Fehlerbehebung

3.5.1 Diagramme

Sie können die Auslastung von NetOp Netfilter überwachen. Wählen Sie hierzu die Optionen Diagramm *Verarbeitete Zugriffe*, Diagramm *Menge der verarbeiteten Daten* oder beide. Auf diese Weise erhalten Sie direkten Einblick in die Serverauslastung. Die Option Diagramm *Verarbeitete Zugriffe* zeigt, wie viele Treffer pro Sekunde momentan durch NetOp Netfilter verarbeitet werden, und die Option Diagramm *Menge der verarbeiteten Daten* zeigt die gesamte Datenmenge an, die durch NetOp Netfilter geleitet wird.

Beide Diagramme werden im gleichen Intervall wie die Informationen in der linken Spalte aktualisiert. Sie können das Aktualisierungsintervall festlegen (siehe Abbildung 34). Der Bereich der Diagrammfenster kann mit Hilfe des Schiebereglers auf der rechten Seite definiert werden.

Siehe hierzu: Statistik

3.6 Die Option Proxy

Diese Option ermöglicht die Konfiguration der Ports für NetOp Netfilter. Außerdem können Sie festlegen, ob der Datenverkehr von NetOp Netfilter über einen externen Proxy geleitet werden soll.

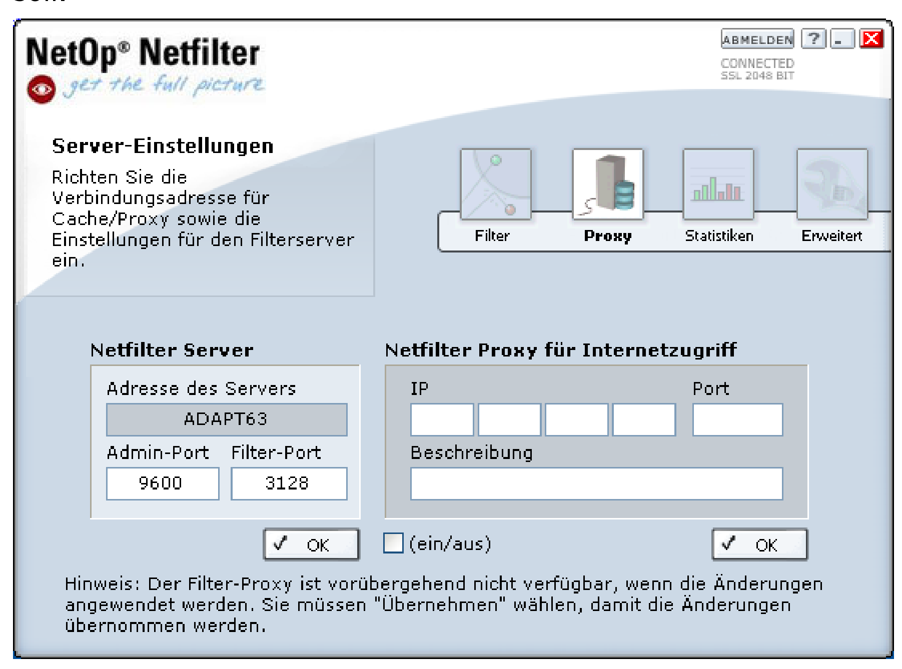


Abbildung 33: Konfigurieren der NetOp Netfilter-Port-Nummern und des externen Proxys.

Siehe hierzu: Proxy, Netfilter-Proxy und Netfilter-Proxy für Internet-Zugriff

3.6.1 Netfilter-Proxy

Hier können Sie festlegen, welcher Port von Browsern für den Internet-Zugriff durch NetOp Netfilter verwendet wird. Standardmäßig ist Port 3128 eingestellt. Dieser Port wird in der Regel für Proxy-Server verwendet. Wenn Sie einen anderen Port verwenden möchten, geben Sie diesen im Feld Filter-Port ein. Wird NetOp Netfilter ohne externen Proxy-Server verwendet, müssen Sie diesen Port nicht ändern. Weitere Informationen zur Nutzung eines externen Proxy-Servers finden Sie weiter unten.

Sie können in NetOp Netfilter auch den Port ändern, der für die Kommunikation mit NetOp Netfilter Admin verwendet wird. Dieser Port ist standardmäßig auf 9600 eingestellt. Wenn Sie einen anderen Port verwenden möchten, geben Sie diesen im Feld Admin-Port ein. Beachten Sie, dass bei nachfolgenden Anmeldungen von NetOp Netfilter Admin aus der neue Port angegeben werden muss. Siehe hierzu auch die Beschreibung im Abschnitt Anmeldung. Die Änderungen an den Port-Einstellungen werden erst nach Klicken auf die Schaltfläche ÜBERNEHMEN wirksam.

Hinweis: NetOp Netfilter ist während der Übernahme der Änderungen für kurze Zeit inaktiv.

Hinweis: Ist der Port 9600 auf dem Computer, auf dem NetOp Netfilter ausgeführt wird, bereits in Verwendung, können Sie den Port für NetOp Netfilter Admin ändern, indem Sie die Textdatei *Data/ProxyAdminPort.cfg* bearbeiten. Diese Datei finden Sie im Ordner von NetOp Netfilter auf dem Filter-Server. Erst nach dieser Änderung können Sie über NetOp Netfilter Admin mit NetOp Netfilter kommunizieren.

Siehe hierzu: Proxy, Die Option Proxy, Netfilter-Proxy für Internet-Zugriff und Fehlerbehebung

3.6.2 Netfilter-Proxy für Internet-Zugriff

NetOp Netfilter kann mit einem externen Proxy-Server verbunden werden (siehe Funktionen). Dies kann nützlich sein, wenn beispielsweise bereits ein Proxy-Server im Netzwerk vorhanden ist. Der Internet-Zugriff erfolgt über den externen Proxy-Server, und NetOp Netfilter filtert den Datenverkehr zwischen dem externen Proxy und den Clients.

Wenn Sie den Datenverkehr über einen externen Proxy-Server leiten möchten, geben Sie dessen IP-Adresse im Feld IP unter *Netfilter-Proxy für Internetzugriff* ein. Ebenso wird der Port des externen Proxy-Servers im Feld Port eingegeben. Darüber hinaus können Sie eine Beschreibung des externen Proxy-Servers eingeben. Diese Informationen werden von NetOp Netfilter nicht verwendet, sondern dienen nur Ihrer Information. (Sie können beispielsweise den DNS-Namen des Proxy angeben.)

Änderungen werden aktiviert, indem Sie auf die Schaltfläche ÜBERNEHMEN klicken, sofern das Kontrollkästchen Ein/Aus markiert ist. Beachten Sie, dass NetOp Netfilter während der Übernahme der Änderungen für kurze Zeit inaktiv ist.

Siehe auch: Proxy, Die Option Proxy, Netfilter-Proxy und Fehlerbehebung

3.7 Fehlerbehebung

In diesem Abschnitt werden einige Probleme beschrieben, die bei der Verwendung von NetOp Netfilter auftreten können. Wenn die nachfolgend aufgeführten Lösungen das Problem nicht beheben, versuchen Sie, den Filter-Server neu zu starten.

Keine Internet-Verbindung über NetOp Netfilter

Ermitteln Sie zunächst, ob vom Filter-Server (Computer, auf dem NetOp Netfilter installiert ist) aus eine Internet-Verbindung besteht. Besteht keine Verbindung, versuchen Sie, diese wiederherzustellen.

Besteht vom Filter-Server aus eine Internet-Verbindung, kann ein Problem mit dem Filter-Port vorliegen, der für die Kommunikation zwischen NetOp Netfilter und den Clients verwendet wird. Möglicherweise wird dieser Port von einem anderen Programm auf dem Server verwendet. In diesem Fall werden Sie von NetOp Netfilter über das Problem informiert, wenn Sie den Filter-Server neu starten. Sie können das Problem anhand einer der beiden folgenden Maßnahmen beheben:

- Konfigurieren Sie einen anderen Filter-Port für NetOp Netfilter und die Clients im Netzwerk, oder
- Konfigurieren (deinstallieren) Sie das andere Programm, so dass dieses nicht mehr den gleichen Port wie NetOp Netfilter belegt.

NetOp Netfilter Admin kann keine Verbindung zum NetOp Netfilter-Server herstellen

Prüfen Sie, ob ein anderer Server den Port verwendet, der für die Kommunikation zwischen NetOp Netfilter-Server und NetOp Netfilter Admin genutzt wird. Standardmäßig wird der Port 9600 verwendet. Sollte dieser von einem anderen Server belegt sein, ändern Sie den Port eines Servers. Sie können die Port-Nummer für NetOp Netfilter in der Textdatei *Data \ProxyAdminPort.cfg* ändern. Diese Datei befindet sich im NetOp Netfilter-Ordner des Filter-Servers. Alternativ können Sie den anderen Server anhalten, sich am NetOp Netfilter-Server über NetOp Netfilter Admin anmelden und unter *Proxy* einen anderen Port als Admin-Port angeben; dazu muss *Erweitert* unter *Erweiterte Einstellungen anzeigen* aktiviert sein).

Unangemessene Seiten werden nicht gesperrt

Starten Sie NetOp Netfilter Admin, und prüfen Sie, ob der Filter aktiv ist (Sie sehen dies auf der Registerkarte *Status*, die beim Programmstart angezeigt wird). Sollte dies nicht der Fall sein, aktivieren Sie den Filter, indem Sie die Registerkarte *Einstellungen* unter Filter auswählen und die Einstellung für Filter ganz deaktivieren ändern.

Prüfen Sie auf der Registerkarte Kategorien unter *Filter*, ob die Kategorie, in der die betreffende Seite gehört, aktiv ist. Ist dies nicht der Fall, aktivieren Sie die Kategorie.

Prüfen Sie, ob die unangemessenen Seiten in der *Liste Immer zulassen* enthalten sind. Ändern Sie die Einstellungen bei Bedarf.

Prüfen Sie, ob der Browser so konfiguriert ist, dass NetOp Netfilter als Proxy-Server verwendet wird. Ist dies nicht der Fall, konfigurieren Sie den Browser mit der Adresse und dem Port für den NetOp Netfilter-Server.

Sind Filter und Browser korrekt konfiguriert, kann das Problem darin bestehen, dass der Filter die betreffenden Seiten falsch einordnet. Sie können diese Seiten in NetOp Netfilter Admin zur Liste Immer sperren hinzufügen. Handelt es sich um ein grundlegendes Problem, können Sie ggf. die Filterempfindlichkeit erhöhen.

Harmlose Seiten werden gesperrt.

Prüfen Sie, ob die entsprechenden Seiten in der *Liste Immer zulassen* enthalten sind. Ändern Sie die Einstellungen bei Bedarf.

In einigen Fällen kann der Filteralgorithmus harmlose Seiten als unangemessen einstufen. Die falsch eingestuften Seiten können in NetOp Netfilter Admin zur Liste Immer zulassen hinzugefügt werden, so dass der Zugriff immer möglich ist. Handelt es sich um ein grundlegendes Problem, können Sie ggf. die Filterempfindlichkeit senken.

Beim Anzeigen einer Seite in Internet Explorer fehlen Bilder

Dieses Problem kann verschiedene Ursachen haben. Wenn Sie Norton Internet Security verwenden und Ihr System nach der Installation von Norton Internet Security auf Internet Explorer 6 aktualisieren, müssen Sie Norton Internet Security erneut installieren.

Wenn Sie Norton Internet Security verwenden, muss das Programm *NetOp Netfilter.exe* vollständigen Internet-Zugriff haben. Diese Einstellung müssen Sie möglicherweise im Administrationsprogramm von Norton Internet Security ändern. Die Einstellung für NetOp Netfilter muss *Alle zulassen* lauten.

Das Problem kann auch dadurch entstehen, dass der Browser für die Kommunikation mit Netfilter nicht HTTP 1.1 verwendet. Im Internet Explorer können Sie diese Einstellung unter *Internetoptionen* auf der Registerkarte *Erweitert* ändern. *Die Option HTTP 1.1 über Proxyverbindungen verwenden* muss ausgewählt sein.

Das Problem kann auch dann auftreten, wenn die Konfiguration von Internet Explorer teilweise geändert wurde, so dass die Kommunikation zwischen Browser und NetOp Netfilter nicht dem Standard entspricht. Der Benutzer kann diese Teile der Konfiguration nicht direkt ändern. Die Änderung wurde möglicherweise durch ein anderes Programm auf dem Computer vorgenommen. Sie können dieses Problem beheben, indem Sie die Registrierung mit der Datei msie_fix.reg aktualisieren. Diese Datei befindet sich im Skriptordner des Installationsverzeichnisses von NetOp Netfilter. Klicken Sie mit der rechten Maustaste auf die Datei, und wählen Sie die Option *Zusammenführen* aus. Dieses Skript stellt außerdem sicher, dass Internet Explorer HTTP 1.1 für die Kommunikation mit Netfilter verwendet.

Bilder können auch dann fehlen, wenn diese von NetOp Netfilter gesperrt wurden, obwohl die Seite selbst freigegeben ist.

Nach dem Aufrufen einer Seite geschieht längere Zeit nichts, dann wird die Seite plötzlich angezeigt

Ohne NetOp Netfilter werden Webseiten nacheinander abhängig von der Geschwindigkeit des Downloads von Texten und Bildern angezeigt. So werden Teile der Seite unmittelbar auf die Seitenanforderung hin angezeigt (indem Sie auf einen Link geklickt oder einen URL eingegeben haben). NetOp Netfilter analysiert die gesamte Seite, bevor diese an den Browser übergeben wird. Auf diese Weise ist die größtmögliche Genauigkeit gewährleistet. Dies kann zu Verzögerungen im Seitenaufbau führen. Nach der Prüfung wird die Seite jedoch umgehend angezeigt, da diese sich im Cache-Speicher von NetOp Netfilter befindet. Die Zeitspanne

zwischen dem Aufrufen einer Seite und dem Anzeigen im Browser dauert bei Verwendung von NetOp Netfilter nur unerheblich länger.

Die Internet-Verbindung wird bei Protokollierung der Benutzernamen sehr langsam

ECLIENT.EXE muss auf allen Client-Computern ausgeführt werden, bevor die Protokollierung der Benutzernamen aktiviert wird. Ist dies nicht der Fall, wird die Internet-Verbindung bei allen Benutzern, auf deren Rechner ECLIENT.EXE nicht ausgeführt wird, sehr langsam.

3.8 Schwarze Listen

Schwarze Listen sind Listen mit Websites, die blockiert werden sollen. Sie können als Kategorien in Netfilter hinzugefügt werden, indem sie in das Verzeichnis Schwarze Listen kopiert werden, das sich im Installationsverzeichnis von Netfilter befindet.

Wenn die Schwarzen Listen von Netfilter geladen wurden (siehe Abschnitt Laden der Schwarzen Listen), müssen sie anschließend aktiviert werden (siehe Abschnitt Filter).

Dateiformat

Schwarze Listen sind einfache Textdateien mit einem URL pro Zeile. Für jede Schwarze Liste muss eine .ini-Datei erstellt werden, die zusätzliche Informationen für Netfilter enthält. Es wird empfohlen, die Schwarze Liste und die .ini-Datei (abgesehen von der Erweiterung) mit dem gleichen Namen zu versehen, etwa "Ihre_Schwarze_Liste.txt" und "Ihre_Schwarze_Liste.ini".

Die .ini-Datei sollte folgende Angaben enthalten:

```
[Config]
blacklistfilename=Ihre_Schwarze_Liste.txt
displayname=Anzeigename Ihrer Schwarzen Liste
description=Beschreibung Ihrer Schwarzen Liste.
uniqueid=UID_IHRESCHWARZELISTE
```

`blacklistfilename` ist der Name der Schwarzen Liste.

`displayname` ist der Name, der in der Verwaltungsoberfläche, in der Protokollanzeige und auf der Sperrseite angezeigt wird.

`description` ist der in der Verwaltungsoberfläche angezeigte Text, der angibt, welche Arten von Websites die Schwarze Liste enthält.

`uniqueid` ist eine einmalige Kennung, die intern von Netfilter verwendet wird. Zwei Schwarze Listen können nicht mit derselben Kennung bezeichnet werden. Um sicherzugehen, dass nur einmalige Kennungen zugewiesen werden, können Sie beispielsweise Ihren Firmennamen in die Kennung mit einbeziehen.

Die Schwarzen Listen laden

Netfilter lädt neue Schwarze Listen automatisch um 02:00 Uhr. Wenn Sie sie zu einem anderen Zeitpunkt laden möchten, führen Sie einfach einen manuellen Neustart des Netfilter-Dienstes aus. Eine Schwarze Liste wird erst aktiv, wenn sie vollständig geladen wurde.

Schwarze Listen auf mehreren Servern einrichten

Netfilter weist Schwarzen Listen numerische Kennungen zu. Werden dieselben Schwarzen Listen auf mehreren Servern eingerichtet und erfolgt der Zugriff über eine zentrale Datenbank, müssen diese Kennungen identisch sein. Netfilter speichert die Kennungen in der Datei categoryids.ini, die sich im Stammverzeichnis von Netfilter befindet.

Wenn neue Schwarze Listen stets in derselben Reihenfolge auf allen Servern eingerichtet werden, sollten ihnen identische Kennungen zugewiesen werden.

So können Sie Schwarze Listen optimal auf mehreren Servern einrichten:

1. Beenden Sie den Netfilter-Dienst auf einem der Server.
2. Kopieren Sie die Schwarzen Listen auf den Server und starten Sie den Netfilter-Dienst neu.

3. Stoppen Sie jeweils auf den übrigen Servern den Netfilter-Dienst, kopieren Sie die Schwarzen Listen auf den Server, kopieren Sie die Datei *categoryids.ini* vom *ersten Server*, und starten Sie den Dienst neu.

Möglicherweise möchten Sie nicht alle Schwarzen Listen auf allen Servern einrichten. Beachten Sie dabei jedoch, dass auf dem Server, von dem Sie die Datei categoryids.ini kopieren, alle Schwarzen Listen installiert sein müssen.

4 Übersicht

Auf die Hilfeseiten können Sie über die Netfilter-GUI zugreifen,

in der sie nach Funktionalität angeordnet sind.

Anmeldung	Filter: Status	Erweitert: Client-Befehle
Proxy-Server	Filter: URL-Listen	Erweitert: Netfilter Admin-Einstellungen
Statistik	Filter: Kategorien	Erweitert: Sperrseite
	Filter: P2P	Erweitert: Cache
	Filter: Chat	Erweitert: Zeitplan
	Filter: Empfindlichkeit	Erweitert: Konten & Berechtigungen
	Filter: Setup	
	Filter: Netzwerk-Setup	
	Filter: Segmente	
	Filter: ACL	

4.1 Anmeldeseite

Um einen Netfilter-Server zu verwalten, müssen Sie sich zunächst anmelden. Die gesamte Kommunikation zwischen dem Verwaltungsprogramm Netfilter Admin und dem Netfilter-Server ist verschlüsselt.

Adresse des Remote-Servers	Geben Sie hier die IP-Adresse und Port-Nummer des Netfilter-Servers ein, den Sie verwalten möchten.
Benutzername des Administrators	Der Standard-Benutzername ist 'admin'. Wenn Sie Ihren Benutzernamen geändert haben, geben Sie den neuen Benutzernamen ein.
Kennwort des Administrators	Das Standard-Kennwort ist 'admin'. Dieses Kennwort muss nach der Erstanmeldung geändert werden, um unbefugten Zugriff auf den Server zu vermeiden.

4.2 Filter

NetOp Netfilter bietet eine Vielzahl von Filtertypen, um die sich laufend ändernden Filteranforderungen zu erfüllen. In den folgenden Abschnitten wird beschrieben, wie Filter eingesetzt werden und was dabei beachtet werden sollte.

Siehe hierzu: Status, URLs, Kategorien, Peer-to-Peer, Chat, Empfindlichkeit, Setup, Netzwerk-Setup, Segmente und Access Control List (Zugangskontrollliste)

4.2.1 Status

Nach der Anmeldung wird die Seite Status angezeigt. Sie können die Seite auch aufrufen, indem Sie unter Filterkonfiguration auf die Registerkarte Status klicken.

Auf der Seite Status wird eine Reihe von Statuselementen angezeigt, die im Folgenden näher erläutert werden. Über die Schaltfläche PROTOKOLL DURCHSUCHEN erhalten Sie außerdem nähere Informationen zum Filterverkehr.

Version	Hierbei handelt es sich um die Versionsnummer und das Veröffentlichungsdatum des Netfilter-Servers.

Hostname und Status des Filter-Servers	Hier werden der Hostname und der Status (aktiviert oder deaktiviert) des Netfilter-Servers angezeigt. Ist der Netfilter-Server deaktiviert, wird ein rotes Warnsymbol angezeigt. Wenn Sie auf dieses Symbol klicken, erfahren Sie, wie Sie den Server wieder in den aktivierten Status zurücksetzen können.
IP-Adresse und Beschreibung des Proxy-Servers für den Internet-Zugang	Hierbei handelt es sich um die IP-Adresse des Proxys, über den der Netfilter-Server auf das Internet zugreift. Daneben finden Sie eine Beschreibung dieses Proxy-Servers. Nicht verwendete Internet-Proxys werden mit der Bezeichnung 'deaktiviert' versehen.
Dienst gestartet	In diesem Feld wird angezeigt, wann der Netfilter-Server gestartet wurde; so können Sie die Betriebszeit abschätzen.
Verarbeitete Byte	Hier wird die Gesamtzahl der Byte angezeigt, die der Netfilter-Server während der Betriebszeit verarbeitet hat.
Ergebnisse	In diesem Feld wird die Gesamtzahl der Zugriffe auf gefilterte Websites sowie die Anzahl der blockierten Zugriffe angezeigt.

Siehe hierzu: Status und Statistik.

Siehe hierzu: Filter, URLs, Kategorien, P2P (Peer-to-Peer), Chat, Empfindlichkeit, Setup, Netzwerk-Setup, Segmente und Access Control List (Zugriffskontrollliste)

4.2.2 URLs

URL-Listen

Die in der Liste Immer zulassen aufgeführten URLs werden den Clients ohne weitere Analysen angezeigt. Die URLs in der Liste Immer sperren werden ohne Abrufen der tatsächlich vorhandenen Daten aus dem Internet, d. h. ebenfalls ohne weitere Analyse, gesperrt. URLs in der Liste der gesperrten URLs können nicht aufgerufen werden, unabhängig von den Einstellungen der Client-Befehle. Auf die gesperrten URLs können nur Clients zugreifen, die mögliche ACL-Regeln erfüllen, nach denen der Internet-Zugriff dieser Clients nicht gefiltert wird.

Einen URL hinzufügen

Um einen neuen URL zu einer der Listen hinzuzufügen, geben Sie einfach den entsprechenden URL in das Textfeld ein, und klicken Sie anschließend auf URL hinzufügen.

Einen URL entfernen

Um einen URL aus einer Liste zu entfernen, markieren Sie den entsprechenden URL durch einfaches Klicken. Klicken Sie anschließend auf die Schaltfläche URL entfernen.

Siehe hierzu: Filter, Status, Kategorien, Peer-to-Peer, Chat, Empfindlichkeit, Setup, Netzwerk-Setup, Segmente und Access Control List (Zugriffskontrollliste)

4.2.3 Kategorien

Auf der Registerkarte Kategorien können Sie festlegen, welche Kategorien der Filter sperren soll. Markieren Sie dazu die gewünschten Kategorien in der Liste links im Bildschirm. Sobald eine Kategorie markiert ist, wird rechts im Fenster eine Beschreibung dieser Kategorie angezeigt.

Siehe hierzu: Filter, Status, URLs, Peer-to-Peer, Chat, Empfindlichkeit, Setup, Netzwerk-Setup, Segmente und Access Control List (Zugangskontrollliste)

4.2.4 P2P (Peer-to-Peer)

Auf der Registerkarte P2P können Sie Peer-to-Peer-Programme sperren, mit denen Software, Musik, Filme usw. im Internet ausgetauscht werden. Die beiden wichtigsten Gründe für das Sperren solcher Anwendungen sind zum Einen die Größe der ausgetauschten Dateien, deren Übertragung aufwändig ist, sowie die Tatsache, dass diese Programm häufig zur unerlaubten Verbreitung von Dateien genutzt werden.

Programmliste

In der Liste links im Fenster können die Peer-2-Peer-Programme ausgewählt werden, die gesperrt werden sollen. Die Standardliste umfasst die gängigsten Peer-2-Peer-Programme; Sie können die Liste jedoch beliebig erweitern.

Wenn Sie mit der rechten Maustaste auf die Liste klicken, wird ein Menü mit den folgenden Funktionen angezeigt:

- Alle Standards sperren. Mit dieser Funktion aktivieren Sie das Sperren aller Programme in der Standardliste.
- Alle Standards zulassen. Mit dieser Funktion deaktivieren Sie das Sperren aller Programme in der Standardliste.
- Alle sperren. Über diese Funktion werden alle Programme in der Liste gesperrt, auch diejenigen, die der Benutzer hinzugefügt hat.
- Alle zulassen. Über diese Funktion wird die Sperre für alle Programme in der Liste aufgehoben, auch für diejenigen, die der Benutzer hinzugefügt hat.

Ein Programm hinzufügen

Wenn Sie ein Programm zur Liste hinzufügen möchten, geben Sie den Namen der EXE-Datei oder den Fenstertitel des Programms ein. Geben Sie im Feld Beschreibung den Namen ein, unter dem das Programm in den Listen angezeigt werden soll. Fügen Sie das Programm hinzu, indem Sie auf REGEL HINZUFÜGEN klicken.

Wenn Sie auf die Schaltfläche mit den drei Punkten rechts neben dem Textfeld des Dateinamens klicken, wird ein Fenster geöffnet, in dem Sie die Datei auswählen können.

Wenn Sie den Dateinamen und den Fenstertitel eingegeben haben, werden alle Programme mit dem entsprechenden Dateinamen oder Fenstertitel gesperrt.

Dateiname und Fenstertitel können auch durch Abgleichen von Teilzeichenfolgen gefiltert werden. Beim Dateinamen werden Programme gesperrt, bei denen der Name der EXE-Datei den angegebenen Text enthält. Wenn Sie beispielsweise "p2p" als Dateinamen festlegen und die Funktion Mit Teilzeichenfolge abgleichen aktivieren, werden die Dateien "p2p.exe", "myp2p.exe" und "p2p program.exe" gesperrt. In der gleichen Weise erfolgt der Zeichenabgleich beim Fenstertitel. Sie sollten diese Funktion jedoch mit Bedacht einsetzen, da Sie sonst schnell ein falsches Programm sperren.

Die Sperrfunktion führt zum Schließen der Programme. Dies kann einige Sekunden dauern. Wenn der Fenstertitel zum Abgleich verwendet wird, wird das Programm nur dann geschlossen, wenn das Fenster aktiv ist.

Ein Programm entfernen

Programme, die vom Benutzer hinzugefügt wurden, können durch Markieren und anschließendes Klicken auf REGEL ENTFERNEN aus der Liste entfernt werden. Die Programme in der Standardliste können nicht entfernt werden.

Siehe hierzu: Filter, Status, URLs, Kategorien, Chat, Empfindlichkeit, Setup, Netzwerk-Setup, Segmente und Access Control List (Zugangskontrollliste)

4.2.5 Chats

Programmliste

In der Liste auf der linken Seite können die zu sperrenden Chat-Typen ausgewählt werden. Ist die Option für Browser-/Online-Chat aktiviert, werden Websites mit Chat-Angeboten gesperrt. Die übrigen Einträge in der Liste umfassen gängige Chat-Programme.

Wenn Sie mit der rechten Maustaste auf die Liste klicken, wird ein Menü mit den folgenden Funktionen angezeigt:

- Alle Standards sperren. Mit dieser Funktion aktivieren Sie das Sperren aller Programme in der Standardliste.
- Alle Standards zulassen. Mit dieser Funktion deaktivieren Sie das Sperren aller Programme in der Standardliste.
- Alle sperren. Über diese Funktion werden alle Programme in der Liste gesperrt, auch diejenigen, die der Benutzer hinzugefügt hat.
- Alle zulassen. Über diese Funktion wird die Sperre für alle Programme in der Liste aufgehoben, auch für diejenigen, die der Benutzer hinzugefügt hat.

Ein Programm hinzufügen

Wenn Sie ein Programm zur Liste hinzufügen möchten, geben Sie den Namen der EXE-Datei oder den Fenstertitel des Programms ein. Geben Sie im Feld Beschreibung den Namen ein, unter dem das Programm in den Listen angezeigt werden soll. Fügen Sie das Programm hinzu, indem Sie auf REGEL HINZUFÜGEN klicken.

Wenn Sie auf die Schaltfläche mit den drei Punkten rechts neben dem Textfeld des Dateinamens klicken, wird ein Fenster geöffnet, in dem Sie die Datei auswählen können.

Wenn Sie den Dateinamen und den Fenstertitel eingegeben haben, werden alle Programme mit dem entsprechenden Dateinamen oder Fenstertitel gesperrt.

Dateiname und Fenstertitel können auch durch Abgleichen von Teilzeichenfolgen gefiltert werden. Beim Dateinamen werden Programme gesperrt, bei denen der Name der EXE-Datei den eingegebenen Text enthält. Wenn Sie beispielsweise "chat" als Dateinamen festlegen und die Funktion Mit Teilzeichenfolge abgleichen aktivieren, werden die Dateien chat.exe, mychat. exe und chat program.exe gesperrt. In der gleichen Weise erfolgt der Zeichenabgleich beim Fenstertitel.

Hinweis: Sie sollten diese Funktion mit Bedacht einsetzen, da Sie sonst schnell ein falsches Programm sperren.

Die Sperrfunktion führt zum Schließen der Programme. Dies kann einige Sekunden dauern. Wenn der Fenstertitel zum Abgleich verwendet wird, wird das Programm nur dann geschlossen, wenn das Fenster aktiv ist.

Ein Programm entfernen

Programme, die vom Benutzer hinzugefügt wurden, können durch Markieren und anschließendes Klicken auf REGEL ENTFERNEN aus der Liste entfernt werden. Die Programme in der Standardliste können nicht entfernt werden.

Siehe hierzu: Filter, Status, URLs, Kategorien, Peer-to-Peer, Empfindlichkeit, Setup, Netzwerk-Setup, Segmente und Access Control List (Zugangskontrollliste)

4.2.6 Empfindlichkeit

Über den Schieberegler auf dieser Seite können Sie die Empfindlichkeit des Filters Ihren Anforderungen anpassen. Dabei können Sie zwischen den drei Grundeinstellungen Niedrig, Normal und Hoch wählen.

Niedrig	Ist die Empfindlichkeitsstufe Niedrig, wird eine weniger strenge Analyse durchgeführt, d. h., es werden möglicherweise mehr Webseiten zugelassen, als durch den Filter festgelegt. Diese Einstellung eignet sich besonders, wenn Sie einen weniger restriktiven Filter verwenden möchten. Die Gefahr, dass unerwünschte Inhalte den Filter passieren, ist höher, wenn die Empfindlichkeit niedrig eingestellt ist, gleichzeitig ist aber das Risiko geringer, dass erwünschte Inhalte ungewollt gesperrt werden.
Normal	Normal ist die Standardeinstellung für den Filter und empfiehlt sich für den normalen Einsatz des Filters.
Hoch	Soll eine strengere Analyse durchgeführt werden, können Sie eine höhere Empfindlichkeit auswählen. Dabei reagiert der Filter sensibler auf unerwünschte Inhalte. Allerdings werden bei dieser Einstellung sehr viele Webseiten als nicht zulässig eingestuft. Die Wahrscheinlichkeit, dass der Filter angemessene Webseiten als unangemessen einstuft, ist höher, gleichzeitig sinkt aber das Risiko, dass unerwünschte Inhalte den Filter passieren.

Siehe hierzu: Filter, Status, URLs, Kategorien, Peer-to-Peer, Chat, Setup, Netzwerk-Setup, Segmente und Access Control List (Zugangskontrollliste)

4.2.7 Setup

Auf dieser Konfigurationsseite können Sie bestimmte Filterfunktionen aktivieren oder deaktivieren.

Allgemein	
Filter ganz deaktivieren	Über diese Option können Sie die Filterfunktion des Netfilter-Servers aktivieren bzw. deaktivieren. Wenn der Filter deaktiviert ist, ermöglicht der Proxy-Server den Clients einen ungefilterten Internet-Zugang.
Konfig.-Sicherung	Hier können Sie eine Konfigurationskopie lokal abspeichern, mit der Sie – bei Bedarf – die Konfiguration wiederherstellen können.
Netzwerk-Setup	Hiermit versenden Sie das aktuelle Setup an andere Server im Netzwerk.
MP3-Analyse	
MP3-Erkennung aktivieren	Wenn diese Funktion aktiviert ist, wird der gesamte MP3-Verkehr in einer Protokolldatei festgehalten. Aktiviert benötigt die MP3-Erkennung mehr Ressourcen. Das Erkennen und Sperren von MP3-Dateien basiert auf Inhaltsanalysen. Das bedeutet, dass der Filter auch MP3-Dateien entdeckt, die sich als andere Formate tarnen. Die Datei MichaelJackson. gif beispielsweise wird erkannt und blockiert, wenn es sich um eine umbenannte MP3-Datei handelt.
Alle MP3-Daten sperren	Der MP3-Verkehr wird gesperrt. Die Funktion MP3-Erkennung erfordert mehr Ressourcen.
Große Dateien	
Erkennung großer Dateien aktivieren	Anhand dieser Funktion können große Dateien, die den Filter passieren, erkannt werden. So kann festgestellt werden, ob solche Dateien übertragen werden. Gleichzeitig wird ein entsprechender Eintrag in der Protokolldatei erstellt. Abhängig von den Gegebenheiten können Unterschiede darin bestehen, wann eine Datei als groß einzustufen ist. Es sollte daher festgelegt werden, ab wann eine Datei als groß betrachtet wird. Die Standardeinstellungen sehen eine solche Einstufung vor, wenn eine Datei mindestens 5.000.000 Byte (ca. 5 MB) groß ist.

Dateien sperren, die größer sind als	Mit dieser Funktion wird die Übertragung von Dateien gesperrt, die die festgelegte Größe überschreiten. Übertragungsversuche werden in der Protokolldatei festgehalten.
Dateiname/-erweit.	
Über die Registerkarte Dateiname/-erweit. können Sie das Sperren mit Regeln konfigurieren, die auf dem Dateinamen basieren.	
Verbreitete Streaming-Medien sperren	Wenn die Option Verbreitete Streaming-Medien sperren aktiviert ist, werden Regeln für die gängigen Streaming-Medien hinzugefügt.
Regeln hinzufügen	Für das Hinzufügen von Regeln stehen drei Methoden zur Auswahl: • Nur Erweiterung. Geben Sie die Erweiterung, z. B. exe oder zip, in das Textfeld ein, und klicken Sie auf REGEL HINZUFÜGEN, um die Erweiterung in die Liste aufzunehmen. Nun werden alle Dateien, die die festgelegte Erweiterung enthalten, gesperrt.
	• Genauer Dateiname. Wenn Sie Dateien mit bestimmten Namen sperren möchten, geben Sie den Dateinamen, wie z. B. 'foo.exe', in das Textfeld ein. Klicken Sie anschließend auf REGEL HINZUFÜGEN – der Dateiname wird in die Liste aufgenommen.
	• Teilweise Übereinstimmung mit Dateiname. Über diese Kategorie können Sie Dateien sperren, deren Namen bestimmte Zeichenfolgen enthalten. Geben Sie die Zeichenfolge, die der Dateiname enthalten soll, in das Textfeld ein, und klicken Sie auf REGEL HINZUFÜGEN, um die Regel hinzuzufügen.
Regeln entfernen	Sie können Regeln entfernen, indem Sie die entsprechende Regel auswählen und anschließend auf REGEL ENTFERNEN klicken.
Protokoll-Setup	
Über diese Option können Sie auswählen, welche Benutzerdaten im Protokoll zusätzlich zu den Adressen der besuchten Seiten registriert werden sollen.	
IP-Adressen protokollieren	Ist diese Option aktiviert, wird die IP-Adresse des Benutzers bei jedem Besuch auf einer Webseite im Protokoll festgehalten.
DNS-Namen protokollieren	Wenn im Netzwerk DNS (Domain Name Service) verwendet wird, können die DNS-Adressen der Clients über diese Funktion protokolliert werden. Die Funktion sollte jedoch nicht aktiviert werden, wenn dieser Service im Netzwerk nicht existiert.
Benutzernamen protokollieren	Wenn das Protokollieren von Benutzernamen aktiviert ist, wird auch im Protokoll festgehalten, welche(r) Benutzer auf dem Computer angemeldet war(en), über den eine bestimmte Webseite aufgerufen wurde. In der Liste der Webseiten, die über den Befehl Seite zulassen und anzeigen aufgerufen wurden, wird der Name des Benutzers angezeigt, der diese Aktion durchgeführt hat.
Clients verwenden gleiche IP-Adresse	Die Funktion "Clients verwenden gleiche IP-Adresse" muss aktiviert werden, wenn mehrere Benutzer dieselbe IP-Adresse verwenden und die Protokollierung von Benutzernamen aktiv ist. Die Datei ECLIENT.EXE muss mit dem im Handbuch beschriebenen Parameter /sharedip ausgeführt werden. Zur Nutzung der gleichen IP-Adresse durch mehrere Benutzer kommt es beispielsweise, wenn Citrix oder Terminal Services verwendet werden oder wenn zwischen den Benutzern und NetOp

	Netfilter ein weiterer Proxy-Server installiert ist. Für eine ordnungsgemäße Protokollierung des Verkehrs bei Nutzung der gleichen IP-Adresse durch mehrere Benutzer ist es unbedingt erforderlich, dass alle Benutzer Internet Explorer als Browser verwenden.

Siehe hierzu: Filter, Status, URLs, Kategorien, Peer-to-Peer, Chat, Empfindlichkeit, Netzwerk-Setup, Segmente und Access Control List (Zugriffskontrollliste)

4.2.8 Netzwerk-Setup

Über die Option Netzwerk-Setup können mehrere Netfilter-Server gleichzeitig verwaltet werden. Dazu müssen Sie die Einstellungen auf einem Server anpassen und diese dann auf die übrigen Server übertragen. Die Server, an die die Einstellungen gesendet werden müssen, werden zur Liste hinzugefügt. Wählen Sie anschließend Übernehmen, um die Einstellungen an die ausgewählten Server zu senden.

Proxy-Einstellungen werden nur an die anderen Server gesendet, wenn die Option Auch Proxy-Einstellungen kopieren aktiviert ist.

Siehe hierzu: Filter, Status, URLs, Kategorien, Peer-to-Peer, Chat, Empfindlichkeit, Setup, Segmente und Access Control List (Zugangskontrollliste)

4.2.9 Segmente

Das Protokoll kann in Segmente unterteilt werden, so dass pro Segment jeweils ein Protokoll erstellt wird. Sie können beispielsweise die einzelnen Abteilungen Ihres Unternehmens als Segmente verwenden. Jedes Segment wird nach IP-Adressen, DNS-Suffixen und Benutzernamen definiert.

Die Unterteilung in Segmente kann nur für zukünftige Protokolle vorgenommen werden; bereits erstellte Protokolle können nicht in Segmente unterteilt werden.

Links im Bildschirm wird eine Liste der Segmente angezeigt. Wenn Sie eines dieser Segmente auswählen, werden auf der rechten Seite die IP-Adressen, DNS-Adressen und Benutzernamen angezeigt, die das Protokoll für dieses Segment enthalten wird.

Sie können die Segmentdefinitionen in einem größeren Fenster anzeigen.

Siehe hierzu: Abbildungen 30 und 31

Segmente hinzufügen

So definieren Sie ein neues Segment:

- Geben Sie unter der Segmentliste den Namen des neuen Segments ein, und klicken Sie auf das +, um das Segment zu erstellen.
- Auf der Registerkarte IP können Sie die IP-Adressen der Computer eingeben, die in dem Segment protokolliert werden sollen. Um ein IP-Adressintervall hinzuzufügen, werden die erste und die letzte IP-Adresse des Intervalls in die beiden dafür vorgesehenen Felder eingegeben. Wenn nur eine einzelne IP-Adresse hinzugefügt werden soll, wird diese in das erste Feld eingegeben. Klicken Sie auf das +, um die Adresse bzw. das Intervall zum Segment hinzuzufügen.
- Auf der Registerkarte DNS können Sie die DNS-Suffixe der Computer eingeben, die in dem Segment protokolliert werden sollen. Geben Sie das Suffix in das Feld ein, und klicken Sie auf das +, um es zum Segment hinzuzufügen. Jetzt werden alle Computer, deren DNS-Name das angegebene Suffix enthält, im selben Segment zusammengefasst. Die eingegebenen DNS-Suffixe werden nur wirksam, wenn das Protokollieren von DNS-Namen aktiviert ist.
- Auf der Registerkarte Benutzername können Sie die Namen der Benutzer eingeben, die in diesem Segment protokolliert werden sollen. Geben Sie den Namen in das Feld ein, und klicken Sie auf das +, um ihn zum Segment hinzuzufügen. Die eingegebenen Benutzernamen werden nur wirksam, wenn die Protokollierung von Benutzernamen aktiviert

ist.

Überschneidungen der einzelnen Segmente sind zulässig. So kann beispielsweise ein Benutzername in mehreren Segmenten eingetragen sein.

Wenn Sie ein Protokoll für einen bestimmten Benutzer erstellen möchten, können Sie ein Segment erstellen, das ausschließlich den Namen dieses Benutzers enthält.

Segmente ändern oder löschen

Wenn Sie ein IP-Intervall, ein DNS-Suffix oder einen Benutzernamen in der Segmentdefinition ändern oder löschen möchten, müssen Sie dieses Element in der Liste auswählen. Anschließend können Sie dieses Element löschen, indem Sie auf ENTFERNEN klicken, oder es ändern, indem Sie den neuen Wert eingeben und auf klicken.

Wenn Sie ein Segment umbenennen möchten, wählen Sie es aus der Liste aus, und geben Sie den neuen Namen ein. Klicken Sie anschließend auf .

Um ein Segment zu löschen, wählen Sie es aus der Liste aus, und klicken Sie auf ENTFERNEN.

Segmentdefinitionen überprüfen

Auf der Registerkarte Segment überprüfen können Sie die Segmente anzeigen, in denen eine IP-Adresse, eine DNS-Adresse oder ein Benutzername protokolliert wird. Geben Sie dazu die Adresse bzw. den Namen ein, wählen Sie den Datentyp, und klicken Sie auf TEST. Die Segmente, in denen die Adresse oder der Name protokolliert werden, sind nun in der Segmentliste markiert.

Siehe hierzu: Segmente einrichten.

Siehe hierzu: Filter, Status, URLs, Kategorien, Peer-to-Peer, Chat, Empfindlichkeit, Setup, Netzwerk-Setup und Access Control List (Zugangskontrollliste)

4.2.10 Access Control List (Zugriffskontrollliste)

Über diese Funktion können Sie einfache Regeln zur Kontrolle der Zugriffsberechtigungen im Netzwerk erstellen. Clients können entweder normalen (also ungefilterten) Zugriff, gefilterten oder keinen Zugriff auf das Internet haben. Die drei Modi werden als NORM, FILT oder VERW gekennzeichnet. Die zusammengestellten Regeln werden als Access Control List oder ACL bezeichnet.

Identifizierung von Clients	Bei der Erstellung von ACL-Regeln werden die IP-Adressen der Clients verwendet, für die die jeweiligen Regeln gelten sollen.
Reihenfolge von ACL-Regeln	Die vom Netfilter-Server verwendeten ACL-Regeln werden im rechten Listenfeld angezeigt. Die Syntax einer ACL-Regel ist – abhängig davon, ob sie sich auf eine oder mehrere IP-Adressen bezieht – 'regel ip' oder 'regel ip-ip'. Spezifische Regeln werden im oberen, allgemeine Regeln im unteren Bereich angezeigt. Das ist wichtig, da für jede eingehende IP die oberste jeweils zutreffende Regel angewendet wird. Wenn beispielsweise der Netfilter-Server eine Homepage-Anfrage vom Client mit der IP 10.2.3.4 erhält, und die aufgelisteten Regeln '10.0.0.0 – 10.255.255.255 VERW' und dann '10.2.3.4 FILT' lauten, wird die Anfrage verweigert, da die erste und daher spezifischere Regel ebenfalls die IP-Adresse des Clients umfasst. Wäre die Reihenfolge der Regeln umgekehrt, d. h. wäre die erste Regel '10.2.3.4 FILT' und die zweite '10.0.0.0 - 10.255.255.255 VERW', würde die Anfrage des Clients als 'gefiltert' weiter verarbeitet. Sie können die Reihenfolge der Regeln verändern, indem Sie auf die beiden Schaltflächen über und unter dem ACL-Listenfeld klicken.
Eine Regel für eine	Wählen Sie den Modus Einzelne IP (das Kontrollkästchen IP-Bereich muss deaktiviert sein). Wählen Sie aus den Regeln NORM

einzelne IP-Adresse hinzufügen	(ungefilterter Zugang), FILT (gefilterter Zugang) oder VERW (Zugang verweigert) die gewünschte Regel aus. Geben Sie anschließend die IP-Adresse des Clients ein, und klicken Sie auf REGEL HINZUFÜGEN. Positionieren Sie die Regel nun an der gewünschten Stelle in der Liste. Regeln für einzelne IP-Adressen sind am spezifischsten und sollten daher oben in der Liste stehen.
Eine Regel für einen IP-Bereich hinzufügen	Wählen Sie den Modus IP-Bereich (das Kontrollkästchen IP-Bereich muss aktiviert sein). Wählen Sie aus den Regeln NORM (ungefilterter Zugang), FILT (gefilterter Zugang) oder VERW (Zugang verweigert) die gewünschte Regel aus. Geben Sie anschließend die erste IP-Adresse in das obere Eingabefeld und die letzte in das untere Eingabefeld ein. Klicken Sie anschließend auf REGEL HINZUFÜGEN. Positionieren Sie die Regel nun gemäß ihrer Priorität. Regeln für IP-Bereiche gelten als allgemeine Regeln und sollten daher unter den Regeln für einzelne IP-Adressen aufgeführt werden.
Eine ACL-Regel entfernen	Wählen Sie durch Klicken mit der linken Maustaste eine Regel aus der Liste aus. Klicken Sie anschließend auf die Schaltfläche REGEL ENTFERNEN bzw. drücken Sie die Schaltfläche Entf auf der Tastatur.
Die ACL-Regelliste testen	Klicken Sie auf die Schaltfläche TEST, um die Funktion der Regel zu überprüfen. Auf dem ACL-Bildschirm wird ein neues Eingabefeld angezeigt. Geben Sie in dieses Feld eine beliebige IP-Adresse ein. Wenn Sie anschließend auf die Schaltfläche IP PRÜFEN klicken, wird die Beurteilung der eingegebenen IP gemäß den aktuellen ACL-Regeln angezeigt.

Siehe hierzu: Filter, Status, URLs, Kategorien, Peer-2-Peer, Chat, Empfindlichkeit, Setup, Netzwerk-Setup und Segmente

4.3 Proxy

Auf dieser Seite können Sie die Server-Einstellungen anzeigen und bearbeiten. Der Netfilter-Server kann entweder direkt oder über einen Internet-Proxy (z. B. Squid) auf das Internet zugreifen.

Hinweis: Änderungen der Einstellungen werden erst dann aktiv, wenn Sie auf die Schaltfläche ÜBERNEHMEN klicken.

Netfilter-Proxy-Einstellungen	
Adresse des Servers	In diesem schreibgeschützten Feld wird der vom Netfilter-Server gemeldete Server-Name angezeigt.
Admin-Port	Hier können Sie den Port des Netfilter-Administrationsservers konfigurieren. Der Port wird verwendet, um Konfigurations- und statistische Daten zwischen dem Netfilter-Server und dem Netfilter Admin-Verwaltungsprogramm auszutauschen. Der Standardwert für diesen Port ist 9600. Wenn der Port von einem anderen Programm oder Server verwendet wird, müssen Sie diesen Wert möglicherweise ändern. • Der gültige Wert muss zwischen 0 und 65535 liegen.
Filter-Port	Diesen Port verwenden Clients für den Internet-Zugang über den Netfilter-Server. Der Standardwert für diesen Port ist 3128. Wenn der Port von einem anderen Programm oder Server verwendet wird, müssen Sie diesen Wert möglicherweise ändern. • Der gültige Wert muss zwischen 0 und 65535 liegen.

Einstellungen des Netfilter-Proxys für den Internet-Zugriff	
Ein-/ Ausschalter	Wenn Sie den Netfilter-Proxy für den Internet-Zugang aktivieren, wird der gesamte Internet-Verkehr über einen externen Proxy-Server geleitet. Dies kann die Integration von NetOp Netfilter in ein Netzwerk, in dem bereits ein Proxy-Server verwendet wird, vereinfachen. Um diese Funktion nutzen zu können, muss ein Proxy-Server aktiviert sein, auf den der Netfilter-Server zugreifen kann.
IP	Hierbei handelt es sich um die IP-Adresse des Computers, auf dem der Proxy-Server installiert ist. • Der gültige Wert besteht aus einer Folge von vier durch Punkte getrennten Zahlen, die zwischen 0 und 255 liegen müssen.
Port	Hierbei handelt es sich um den Port, auf dem der Proxy-Server ausgeführt wird. • Der gültige Wert muss zwischen 0 und 65535 liegen.
Beschreibung	Hier können Sie eine beliebige Beschreibung des Proxy-Servers eingeben, wie z. B. den Hostnamen und die Modellnummer. • Sie können jede beliebige Zeichenfolge eingeben.

4.4 Statistik

Wenn das Verwaltungsprogramm Netfilter Admin mit dem Netfilter-Server verbunden ist, erhält es vom Server fortlaufend statistische Echtzeitdaten. Auf der Seite Statistik können Sie diese Daten in Form von Zahlen und Diagrammen abfragen.

Update-Intervall

Wählen Sie aus einem der folgenden Update-Intervalle: Häufig aktualisieren, ½ Sek., 1 Sek. und 5 Sek. Die unterschiedlichen Intervalle bestimmen, wie oft der Netfilter-Server aktualisiert wird.

Numerische Daten

Ca. Treffer/ Sek	Anzahl verarbeiteter Treffer pro Sekunde.
Max. Treffer/ Sek	Anzahl Treffer, die pro Sekunde verarbeitet werden.
Gesamttreffer	Gesamtzahl der Treffer, die der Server für alle Clients verarbeitet hat.
Zugelassene Treffer	Anzahl der Treffer, die der Filter zugelassen hat und die bei den Clients angezeigt wurden.
Gesperrte Treffer	Anzahl der Treffer, die gesperrt und daher vom Netfilter-Server zurückgehalten wurden.
Offene Sitzungen	Anzahl der aktiven Client-Anfragen.
Durchschn. Bytes/Sek	Anzahl der Byte, die durchschnittlich pro Sekunde vom Server verarbeitet werden.
Max. Kb/Sek	Maximale Anzahl der Byte, die pro Sekunde vom Server verarbeitet werden.
Gesamt Kb	Gesamtzahl der Byte, die der Server verarbeitet hat.

Hinweis: Die Maßeinheit Byte ändert sich mit zunehmender Größe von KB zu MB.

Das Diagramm 'Treffer/Sek.'

Dieses Diagramm zeigt die Anzahl der Treffer (oder Anfragen) an, die der Server momentan pro Sekunde verarbeitet. Die graue Kurve veranschaulicht diese Anzahl. Ist das Diagramm leer, werden keine Daten verarbeitet. Die Anzahl der durchschnittlich pro Sekunde verarbeiteten Daten wird ebenfalls in Form eines Diagramms mit grauem Hintergrund angezeigt.

Das Diagramm 'Bytes/Sek.'

Dieses Diagramm zeigt die Anzahl der Byte an, die der Server momentan pro Sekunde verarbeitet. Die graue Kurve veranschaulicht diese Anzahl. Ist das Diagramm leer, werden keine Daten verarbeitet. Die Anzahl der durchschnittlich pro Sekunde verarbeiteten Byte wird ebenfalls in Form eines Diagramms mit grauem Hintergrund angezeigt.

Siehe hierzu: Status.

4.5 Erweiterte Einstellungen

Klicken Sie auf die Schaltfläche Erweitert, um auf die erweiterten Einstellungen zuzugreifen.

Siehe hierzu: Erweitert, Interaktive Client-Befehle, Netfilter Admin-Einstellungen, Sperrseite, Cache, Zeitplan und Konten und Berechtigungen

4.5.1 Interaktive Client-Befehle

Der Netfilter-Server stellt die interaktiven Client-Befehle bereit. Je nach Server-Version kann die Anzahl der verfügbaren Befehle variieren. Zum Zeitpunkt der Erstellung ist lediglich ein Befehl verfügbar.

Client-Befehle aktivieren/ deaktivieren	Wenn Sie die Befehle verwenden möchten, aktivieren Sie das Kontrollkästchen Interaktive Client-Befehle auf der gesperrten Seite aktivieren. Wenn Sie einen bestimmten Client-Befehl aktivieren möchten, zu dessen Ausführung die Clients auf der gesperrten Seite berechtigt sein sollen, wählen Sie den betreffenden Befehl einfach aus der Liste aus und klicken Sie auf die Schaltfläche AKTIVIEREN. Zum Deaktivieren eines Befehls klicken Sie entsprechend auf die Schaltfläche DEAKTIVIEREN.
Der Befehl 'Seite zulassen und anzeigen'	Über diesen Befehl können die Benutzer eine Webseite, die gesperrt ist, anfordern; dazu müssen sie eine Schaltfläche auf der gesperrten Seite anklicken. Ein Text auf der gesperrten Seite weist den Benutzer darauf hin, dass der Zugriff auf diese Seite im Protokoll registriert wird.
Der Befehl 'Sperr-Seite deaktiviert'	Wenn dieser Befehl aktiviert ist, werden die besuchten Seiten nicht gesperrt, der Zugriff wird jedoch im Protokoll festgehalten.

4.5.2 Netfilter Admin-Einstellungen

Auf dieser Konfigurationsseite können Sie die Einstellungen des Verwaltungsprogramms ändern.

Erweiterte Einstellungen anzeigen	Wenn dieses Kontrollkästchen aktiviert ist, werden die erweiterten Einstellungen angezeigt. Normalerweise müssen diese Einstellungen nicht geändert werden.
Einstellungen für Datenbankverbindung	Sie können die von NetOp Netfilter verwendete Datenbank ändern. Klicken Sie dazu auf Setup. Geben Sie in das nun angezeigte Fenster IP-Adresse, Benutzername, Kennwort und den Namen der

	Datenbank ein. Wenn Sie die Datenbank nicht verwenden möchten, lassen Sie diese Parameter offen. Die Daten werden dann in lokalen Protokolldateien auf dem Netfilter-Server registriert.
Zeitplan mit täglichem Zeitlimit verwenden	Mit Hilfe eines Zeitplans können für die unterschiedlichen Wochentage und Tageszeiten verschiedene Filtereinstellungen verwendet werden. Aktivieren Sie die Funktion Zeitplan mit täglichem Zeitlimit verwenden und klicken Sie anschließend auf Zeitplan, um Zeitpläne zu erstellen.
Klickgeräusche beim Betätigen von Schaltflächen	Sie können die Klickgeräusche für Schaltflächen deaktivieren.
SSL-Verbindung überprüfen	Wenn Ihre Internet-Verbindung zum Server nicht durchgehend verfügbar ist, d. h., wenn Sie keine Standleitung, sondern ein Modem o. ä. verwenden, kann diese Funktion von Vorteil sein. Wenn die Überprüfungsfunktion aktiviert ist, sendet das Verwaltungsprogramm in regelmäßigen Abständen eine Verfügbarkeitsanfrage an den Server ('Are-you-alive'). Antwortet der Server nicht, erhalten Sie eine Nachricht, dass die Verbindung unterbrochen ist. Alle bis dahin geänderten Einstellungen sind möglicherweise nicht gespeichert, da keine Verbindung mehr zum Server besteht.
	Für die Durchführung dieser Tests können Zeitintervalle festgelegt werden. Wenn Sie sich über ein Modem einwählen, ist ein kurzes Intervall sinnvoll. Verwenden Sie hingegen eine schnelle und zuverlässige Verbindung, kann eine Überprüfung in größeren Abständen geeigneter sein.
Automatische Abmeldung	Sie können die automatische Abmeldung des Programms beim Minimieren des Programmfensters einstellen. Aktivieren Sie dazu diese Funktion.
Benutzernamen und Kennwort ändern	Wenn Sie Ihren Benutzernamen und/oder Ihr Kennwort ändern möchten, geben Sie die neuen Daten in die entsprechenden Textfelder ein. Durch Klicken auf OK erfahren Sie, ob der Vorgang erfolgreich war. Wenn Sie die Daten ändern, ändert sich automatisch auch die Verschlüsselung zwischen dem Verwaltungsprogramm und dem Server.

Warnung: Bei Verlust der Anmeldedaten können Sie keine Verbindung zum Server zu Verwaltungszwecken mehr herstellen!

Siehe hierzu: Netfilter Admin-Einstellungen.

4.5.3 Sperrseite

Sprache der Sperrseite

Die Funktion Sperrseite ist in diversen Sprachen verfügbar. Wählen Sie die gewünschte Sprache für Ihre Benutzer aus der Liste aus.

HTML-Sperrseite anpassen

Sie können die Standard-Sperrseite durch eine benutzerdefinierte Seite ersetzen, die auf einer HTML-Vorlage basiert. Importieren Sie dazu die Vorlage über die Option Vorlage importieren..., und aktivieren Sie die Option HTML-Vorlage verwenden. Die Vorlage muss eine HTML-Seite

sein, die die folgenden Tags enthält:

HTML-Tag	Beschreibung	
[%filter-report%]	Die Zeile, die dieses Tag enthält, wird durch die Meldung ersetzt, dass die betreffende Seite gesperrt wurde, und es werden Links für die ausgewählten Client-Befehle hinzugefügt.	
[%filter-message %]	Die Zeile, die dieses Tag enthält, wird durch die Meldung ersetzt, dass die gewünschte Seite gesperrt wurde.	
[%image-view src="IMAGEURL"%]	Die Zeile mit diesem Tag wird durch die Schaltfläche Anzeigen ersetzt. Die am angegebenen Ort abgespeicherte Abbildung (IMAGE URL) wird für die Schaltfläche verwendet. Die Schaltfläche wird nur dann angezeigt, wenn der Client-Befehl Seite zulassen und anzeigen aktiviert ist.	
[%image-back src="IMAGEURL"%]	Die Zeile mit diesem Tag wird durch die Schaltfläche Zurück ersetzt. Die am angegebenen Ort abgespeicherte Abbildung (IMAGE URL) wird für die Schaltfläche verwendet.	
[%block-category %]	Dieses Tag wird durch die Kategoriebezeichnung für die betreffende Seite ersetzt.	
[%powered-by%]	Dieses Tag wird durch folgenden Text ersetzt:	
	Powered by	NetOp Netfilter (c) 2007, Danware A/S
	{%blocked-url %}	Dieses Tag wird durch den gesperrten URL ersetzt.
	{%timestamp %}	Dieses Tag wird durch die Anzeige des Zeitpunkts, zu dem die Seite gesperrt wurde, ersetzt.

Hinweis:
[%...%] Diese Tags müssen allein in eine Zeile gesetzt werden.
{%...%} Diese Tags können beliebig im Text eingesetzt werden.

4.5.4 Cache

Zurücksetzen NetOp Netfilter speichert die aufgerufenen Seiten in einem Cache-Speicher, um den erneuten Zugriff auf die Seiten zu beschleunigen. Verwenden Sie diese Funktion, um den Inhalt des Cache zu löschen.

4.5.5 Zeitplan

Mit NetOp Netfilter können Sie bestimmte Einstellungen auf Grundlage eines Zeitplans programmieren. Zu diesen Einstellungen zählen der Internet-Zugriff bestimmter Segmente, die Aktivierung des Filters und die Inhalte, die der Filter sperren soll.

Wenn kein Zeitplan erstellt wurde, werden die im Hauptfenster (siehe vorherige Abschnitte) festgelegten Einstellungen verwendet. Wurden im Zeitplan Blöcke definiert, haben diese Vorrang vor den Einstellungen im Hauptfenster.

Einen Block zum Zeitplan hinzufügen	Sie können einen Block festlegen und Einstellungen dafür im Zeitplan vornehmen. Klicken Sie dazu auf ein Zeitfeld, um den Beginn des Zeitraums zu markieren, und ziehen Sie die gedrückte Maustaste über den gewünschten Zeitraum. Klicken Sie nach dem Markieren des Zeitraums mit der rechten Maustaste auf den markierten Bereich, und

	wählen Sie die Option Hinzufügen... aus. Der Inhalt des Fensters wechselt dann zur Einstellungssteuerung.
Einstellungen für einen Block auswählen	Über die Einstellungssteuerung können Sie Anfang und Ende des Zeitraums anpassen und auswählen, an welchen Wochentagen die gewählten Einstellungen gelten sollen. Sie können außerdem auswählen, auf welche Segmente diese Einstellungen angewendet werden sollen. Dies bedeutet, dass für verschiedene Segmente zur gleichen Zeit unterschiedliche Einstellungen gelten können.
	Die Einstellungen für den gewählten Zeitraum können in der Liste am unteren Fensterrand bearbeitet werden. Weitere Informationen zu diesen Einstellungen finden Sie im vorherigen Abschnitt.
	Wenn Sie die zu verwendenden Einstellungen und Segmente sowie den Zeitraum angegeben haben, klicken Sie auf ÜBERNEHMEN. Auf diese Weise gelangen Sie zurück zum Zeitplan, wo Sie neue Blöcke hinzufügen, die Einstellungen vorhandener Blöcke ändern und Blöcke löschen können.
Blöcke bearbeiten und löschen	Um die Einstellungen für einen Block zu ändern, rufen Sie das Kontextmenü des entsprechenden Blocks mit der rechten Maustaste auf, und klicken Sie auf Bearbeiten… Wenn Sie einen Block aus dem Zeitplan entfernen möchten, klicken Sie im Kontextmenü auf Löschen.
Den Zeitplan für ein Segment anzeigen	Wenn Sie den Zeitplan für ein bestimmtes Segment anzeigen möchten, wählen Sie im oberen Fensterbereich das betreffende Segment im Listenfeld aus.

4.5.6 Konten und Berechtigungen

Sie können verschiedene Benutzerkonten erstellen und verschiedenen Benutzergruppen von Netfilter Admin unterschiedliche Rechte zuweisen.

Im oberen Fensterbereich wird eine Liste der Benutzergruppen angezeigt. Im unteren Bereich wird angezeigt, zu welcher Gruppe welcher Benutzer gehört.

Gruppen	Klicken Sie auf Hinzufügen, um eine neue Gruppe zu erstellen. In dem nun angezeigten Fenster können Sie den Namen, eine Beschreibung und die Berechtigungen für die Gruppe eingeben. Dieses Fenster können Sie zu einem sp äteren Zeitpunkt öffnen, indem Sie die Gruppe auswählen und auf Eigenschaften klicken. Gruppen, denen keine Benutzer zugewiesen wurden, können über Entfernen gelöscht werden. Sie können einer Gruppe die Berechtigung zur Änderung der Listen Immer sperren und Immer zulassen oder einen uneingeschränkten Zugriff auf alle Einstellungen zuweisen.
Benutzer	Neue Benutzer können Sie über die Schaltfläche Hinzufügen unterhalb der Liste der Benutzerkonten hinzufügen. In dem angezeigten Fenster können Sie Name, Kennwort, Gruppenzugehörigkeit usw. auswählen. Soll das Konto automatisch nach einem festgelegten Zeitraum ablaufen, aktivieren Sie Das Konto ist gültig bis, und geben Sie ein Datum und einen Zeitpunkt ein. Analog zu den Gruppeneinstellungen können über Eigenschaften die Benutzereigenschaften angezeigt und über Entfernen einzelne Benutzer gelöscht werden.

Siehe hierzu: Konten & Berechtigungen.

Index